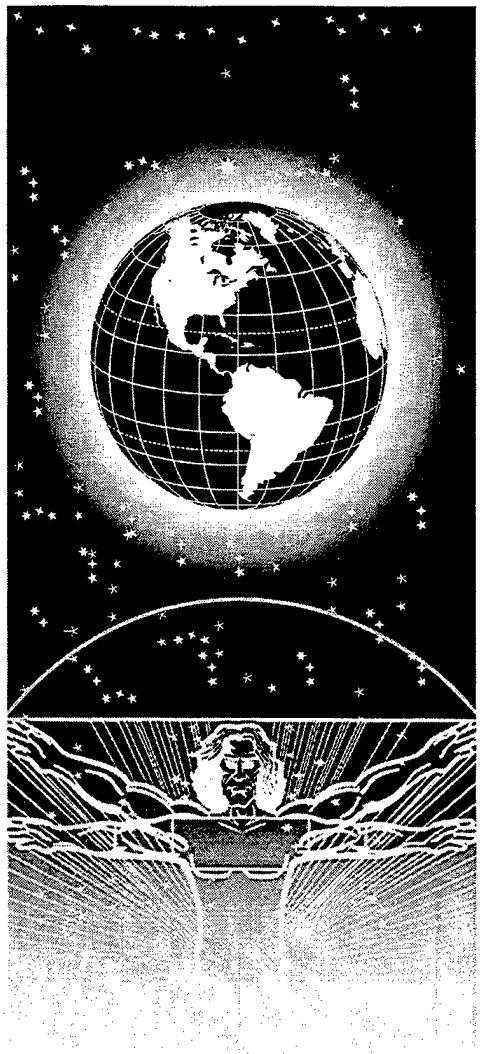
AFRL-HE-WP-TR-1999-0234



UNITED STATES AIR FORCE RESEARCH LABORATORY

DECISION-MAKING UNDER ATTACK: INFORMATION WARFARE

Jeff Bradford
Elisabeth Fitzhugh

ADROIT SYSTEMS, INC.
5100 SPRINGFIELD STREET
SUITE 210
DAYTON OH 45431

JUNE 1999

INTERIM REPORT FOR THE PERIOD 1 MAY 1998 TO 30 JUNE 1999

Human Effectiveness Directorate
Crew System Interface Division
2255 H Street
Wright-Patterson AFB OH 45433-7022

NOTICES

When US Government drawings, specifications, or other data are used for any purpose other than a definitely related Government procurement operation, the Government thereby incurs no responsibility nor any obligation whatsoever, and the fact that the Government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data, is not to be regarded by implication or otherwise, as in any manner licensing the holder or any other person or corporation, or conveying any rights or permission to manufacture, use, or sell any patented invention that may in any way be related thereto.

Please do not request copies of this report from the Air Force Research Laboratory. Additional copies may be purchased from:

National Technical Information Service
5285 Port Royal Road
Springfield, Virginia 22161

Federal Government agencies and their contractors registered with the Defense Technical Information Center should direct requests for copies of this report to:

Defense Technical Information Center
8725 John J. Kingman Road, Suite 0944
Ft. Belvoir, Virginia 22060-6218

TECHNICAL REVIEW AND APPROVAL

AFRL-HE-WP-TR-1999-0234

This report has been reviewed by the Office of Public Affairs (PA) and is releasable to the National Technical Information Service (NTIS). At NTIS, it will be available to the general public.

This technical report has been reviewed and is approved for publication.

FOR THE COMMANDER

MARIS M. VIKMANIS
Chief, Crew System Interface Division
Air Force Research Laboratory

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	June 1999	Interim, 1 May 1998 - 30 June 1999

4. TITLE AND SUBTITLE
Decision-Making Under Attack: Information Warfare

5. FUNDING NUMBERS
C: F41624-94-D-6000
P: 62202F
PR: 7184
TA: 10
WU: 46

6. AUTHOR(S)
Bradford, Jeff; Fitzhugh, Elisabeth

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Adroit Systems, Inc.
5100 Springfield Street
Suite 210
Dayton, OH 45431

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory
Human Effectiveness Directorate
Crew System Interface Division
Air Force Materiel Command
Wright-Patterson AFB, OH 45433-7022

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-HE-WP-TR-1999-0234

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

In order to meet new warfare challenges, decision-makers must learn from past military experience and adapt new, practical models to predict Information Warfare (IW) attacks or events. This study reviews critical aspects of the decision-making process and techniques used to alter decision-making, explores how business process reengineering (BPR) methods may be utilized to optimize IW operations, and provides a premise for future testing. It demonstrates the need for those who conduct IW and information operations to incorporate a basic understanding of perceptual processing and adversarial decision-making processes into future IW operational planning.

The report discusses the OODA Loop activity cycle and its utility and shortcomings as a decision-making model and extends the basic OODA Loop activity cycle to incorporate a core set of elements (technology, emotion, culture, and knowledge) which mediate perceptual processes and influence decision-making. The core elements (or TECK model), when merged with the OODA Loop activity cycle, form an iterative, multi-loop, integrated model of the operational decision-making process. The report recommends focused, human factors-oriented research to improve understanding of the TECK elements and their effect on decision-making as a prerequisite to the design of effective predictive analytical tools.

14. SUBJECT TERMS
Adversarial Decision-Making, Decision Making Aids, Modeling, Predictive Models, OODA Loop, Information Operations, Information Analysis, Information Warfare

15. NUMBER OF PAGES
68

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UNL

This page intentionally left blank.

PREFACE

Information Warfare (IW) has become a dominant factor in the planning and execution of military operations. This paper is designed to review some of the critical aspects of the decision-making process, the methodologies and techniques to alter decision-making and how IW operations can be optimized for future operations. The information provided in this document is not based on scientific fact or testing, but is an analytical opinion and a premise for future testing. The author is a former military analyst with over 20 years of experience in intelligence and its role in support of military operations. It is the author's intent to demonstrate the need for those who conduct IW and information operations (including those who deal in the key sub-components of camouflage, concealment and deception, and psychological warfare) to incorporate a basic understanding of the adversary's decision-making and perception processes into operational planning, prior to an IW engagement.

The author makes the following assumptions: that the terms decision-making, perception, culture, technology, knowledge and emotion—though they have many connotations and definitions (i.e., numerous dissertations and writings exist to define and defend these concepts)—are the concepts as generally understood and will not be explored at this time.

The opinions expressed in this document reflect the views of the author and not necessarily the views of government or of the Air Force Research Laboratory.

This effort was performed by Adroit Systems, Inc., for the Information Analysis and Exploitation Branch, Crew System Interface Division, Human Effectiveness Directorate of the Air Force Research Laboratory (AFRL/HECA), Wright-Patterson AFB, OH, under contract F41624-94-D-6000, Work Unit 71841046, "Crew Systems for Information Warfare." Work was accomplished under the direction of prime contractor, Logicon Technical Services, Inc.; Mr. Donald Monk was the contract monitor.

The author expresses appreciation to Mr. Gilbert Kuperman (AFRL/HECA), Work Unit Manager, who initiated and guided the effort. Thanks are also due to Mr. Robert L. Stewart of LTSI for his support as project manager.

TABLE OF CONTENTS

Page

LIST OF FIGURES v

LIST OF TABLES vi

INFORMATION WARFARE—AN INTRODUCTION 1

THE DECISION-MAKING PROCESS 4

METHODOLOGIES FOR ALTERING OR INFLUENCING THE DECISION-MAKING PROCESS 20

IW MODELING AND PLANNING TOOLS 30

CONCLUSION 46

REFERENCES 48

ACRONYM LIST 51

GLOSSARY 53

LIST OF FIGURES

Figure **Page**

1. The OODA Loop. 4
2. Linear OODA Loop Depiction. 8
3. Multiple OODA Loop Interactions. 9
4. OODA Loop Influences. 10
5. The TECK Model. 13
6. Detail of the OODA Loop Sketch: Orientation (Spinney, 1997) 16
7. The OODA Loop Set Askew. 20
8. Deception Flow Model. 24
9. The Shewhart Cycle. 31
10. The Continuous Improvement Process (adapted from Holmes, 1994). 31
11. Force Field Analysis. 33
12. Ishikawa "Fishbone" or Cause and Effect Diagram. 34
13. Somalia Event Fishbone. 35
14. Notional Run Chart of Seasonally-Based Vehicle Activity 37
15. Deception Matrix. 38
16. TECK Matrix. 39
17. Decision Tree Showing Decision Branches With Associated Probabilities. 41
18. Course of Action Development (Murphy et al., 1996). 43
19. Human and Technology Interaction—Decision-Making Matrix for the Information Battlespace 44
20. Decision-Making Matrix for Process Modeling Tools. 45

LIST OF TABLES

Table		Page
1.	OODA Loop Modes	8
2.	Modeling Tools (adapted from Holmes, 1994)	32
3.	Somalia Event Matrix	36

INFORMATION WARFARE—AN INTRODUCTION

The world is in the midst of the information age. History shows that each new age develops its accompanying new weapons and new warfare techniques. The information age affects all aspects of modern life, but none more dramatically than military operations. New terminology, such as Information Warfare (IW) and Information Protect (IP), dominates the conversations and guides the thought processes of many military and civilian leaders. The Department of Defense (DoD) defines information warfare as "[i]nformation operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries" (*Joint Pub 1-02,* 1999). It is also defined as actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems and computer-based networks, while defending one's own information, information-based processes, information systems, and computer-based networks (*AFDD 1*, 1997). Information Superiority is considered to be one of the six core competencies of modern warfare; the other competencies include Air and Space Superiority, Global Attack, Precision Engagement, Rapid Global Mobility, and Agile Combat Support (*Joint Vision 2010,* 1996). Information Superiority is that degree of dominance in the information domain which permits the conduct of operations without effective opposition (*Joint Pub 1-02*). New methods of combat emphasizing IW offensive and defensive operations are being devised, and billions of tax dollars are being invested. Capitalizing both on lessons learned and on those "tried and true" techniques used throughout history to manipulate the adversary's decision-making process, IW has itself become the ultimate weapon of the information age.

Information Operations (IO) are those methods, actions, or techniques utilized to conduct either offensive or defensive information warfare. IO can affect an array of political, economic, civilian, or military targets. A televised news conference with an important dignitary could be altered to change its content. An economy could be sabotaged by reducing international confidence in a nation's currency or by causing an adversary to default on payments. Access to critical research and development facilities could be interfered with or have data removed or altered. Satellite communications could be terminated. Strategic information operations, waged independently, could cause an adversary to lose faith in his own data management systems—greatly increasing confusion and decreasing the ability to control assets. On an operational level, interference with enemy data management systems could create damaging time delays in the

enemy's ability to make and implement decisions. On the tactical level, the use of IW techniques would complement other tactical systems to reduce danger to friendly forces and increase chances for success.

IW opens new avenues for the conduct of political-military operations. On the low level of the conflict spectrum, covert intrusion into an opponent's command and control system may provide unique insight into their political intentions and decision-making process. To help the Air Force identify the means for conducting IW operations, General Ronald Fogleman (former Air Force Chief of Staff), in *Cornerstones of Information Warfare*, defines six forms or categories of IW (Widnall & Fogleman, 1996). These six categories of IW are the key modifiers of the decision-making process.

Psychological Operations: Use information to affect the enemy's reasoning.

Electronic Warfare: Deny accurate information to the enemy.

Military Deception: Mislead the enemy about our capabilities or intentions.

Physical Destruction: Affect information system elements through the conversion of stored energy to destructive power. The means of physical attack range from conventional bombs to electromagnetic pulse weapons.

Security Measures: Seek to keep the adversary from learning about our military capabilities and intentions.

Information Attack: Directly corrupt information without visibly changing the physical entity within which it resides.

The information age has truly expanded the realm within which we think and operate. This vast expansion of information incorporates all areas of communication, computers, and data. The military's primary concern no longer remains centered on supporting traditional warfighting bastions. The general population, or civilians, may be affected directly or by collateral damage during attacks on the "Information Battlespace" or in non-specific information warfare attacks. The battlespace, or "infospace," comprises the environment in which humans and their machines operate. In the past, many methods, such as camouflage and deception measures, have been used to counter or embellish standard warfare attacks. Brennan and Ellis (1996) break down IW into prime "functional areas of perception management, information degradation or denial, and information exploitation." These functional areas, to an extent, mirror the traditional warfare

techniques of camouflage, concealment, denial, and deception (CCDD) and psychological warfare techniques. In order to meet new warfare challenges, decision-makers must learn from past military experience and adapt new, practical models to predict IW attacks or events.

The most complicated operating system within the infospace, or battlespace, is the human mind. For centuries philosophers, theologians, anthropologists, mathematicians, psychologists, and others have tried to define how, within the decision-making process, knowledge, logic, trust, and faith operate and interact. To understand or predict the adversary's thought process or anticipated action has been a priority for military leaders since long before the writings of Sun Tzu (400-320 BCE). Military leaders have sought oracles, psychics, and sorcerers to predict both enemy plans and actions. The process of prediction analysis has become one of the most crucial components of intelligence preparation of the battlespace (IPB). IPB is "[a]n analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive database for each potential area in which a unit may be required to operate. The database is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and presents it in graphical form. Intelligence preparation of the battlespace is a continuing process" (*Joint Pub 1-02,* 1999). "Intelligence preparation of the battlefield can reduce vulnerability to enemy actions by describing enemy courses of action so that they can be countered, forestalled, or exploited" (*AFM 1-1, Vol. II,* 1992, p. 18). Exploiting IPB-derived data enables IW operations to be targeted at the military or political decision-makers. To capitalize on frailties of the human mind is the primary goal of IW actions. IO attacks prey on the developed trust and reliance of system users in and on their infospace, and they exploit that relationship. That is, an operator who regularly receives a standard signal or display will tend to believe in the legitimacy of all such signals and displays. This tendency may be exploited through the injection of false data. The operator will be likely to report false data as real data. Such an IW tactic may prove to be more devastating than a direct attack that actually shuts down the system or destroys data. Destructive attacks (hard kills) are more readily apparent. Operators and decision-makers who are aware of an attack can take corrective action. But the subtle attack, or soft kill, that manipulates data and perceptions may produce a longer term effect on the decision-making process, as it goes unnoted and its effects proliferate. This report reviews the key components of the decision-making process, including the methods commonly used to exploit that process and the planning tools that help model it.

THE DECISION-MAKING PROCESS

The decision-making (DM) process consists of the set of steps taken to conduct a discrete thought process or to compose a complete plan of action, from inception to conclusion. Naturalistic decision-making (NDM) refers to how experienced decision-makers apply their experience in the field (Klein, 1997). DM studies in the military domain are usually pragmatic, and NDM-focused. While studying the DM process in Air Force pilots, Col John Boyd developed a descriptive four-phase model that he termed the OODA Loop (see Figure 1). The OODA Loop has become a paradigm of the decision-making process in operational settings, including operational IW. The OODA Loop takes its name from the activity sequence, *Observe*, *Orient*, *Decide*, *Act*; the sequence is always presented in action verbs and represents the phases through which the decision-maker passes in responding to a stimulus event (Boyd, 1987).

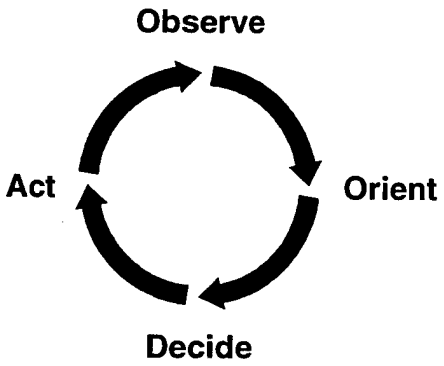


Figure 1. The OODA Loop.

In the following extract, Whitaker and Kuperman capture the essence of the OODA Loop as defined by Boyd.

> ... The following describes the four individual phases comprising a unit OODA Loop with respect to an individual subject:
>
> *Observe phase.* In the Observe (Ob) phase of an OODA Loop, the subject, operating within his/her role, engages phenomena in the environment within which he/she pursues the process. Observation consists of the subject's transformation of

phenomena into a set of data. The Observe phase concludes at the point that the subject begins integrating this data into his/her knowledge base.

Orient phase. In the Orient (Or) phase of an OODA Loop, the subject, operating within his/her role, engages data deriving from observation. Orientation consists of distilling information ("any difference that makes a difference"—Bateson, 1987) from the data stream and integrating that information along with prior facts and understandings into a coherent state of situational knowledge. The Orient phase concludes at the point that the subject achieves this coherent state. Note that the criterion for Orient phase completion is a "coherence" of situational knowledge, not a "completeness" or "accuracy" of situational knowledge.

Decide phase. In the Decide (D) phase of an OODA Loop, the subject, operating within his/her role, engages situational knowledge deriving from orientation. Decision consists of evaluating this situational knowledge, projecting its ramifications for the process, focusing on a set of chosen ramifications, and selecting action(s) appropriate to that focus (a plan). The Decide phase concludes at the point that the subject moves from reflection on to enactment of the selected action(s).

Act phase. In the Act (A) phase of the OODA Loop, the subject, operating within his/her role, engages the process environment with respect to the plan deriving from decision. Action consists of transforming the abstract plan into instrumental behavior. The Act phase concludes at the point that the subject completes or interrupts realization of the plan and begins observing the newly-changed state of the process environment. (Whitaker & Kuperman, 1996, p. 53)

This OODA Loop model comprehensively defines the basic, "bare bones" decision-making process. Even though Boyd contends that all decision actions are similar and can be expressed with the OODA Loop, three separate decision variants or modes can be observed or construed.

Deliberate OODA Acts (planned actions). Deliberate or premeditated decision-making processes tap all perceptual senses to determine a logical path or solution. Key objectives, goals, or specific achievements are defined. The amount of planning involved requires adequate preparation time and careful consideration of contributing factors and risk mitigation. Timing for deliberate acts can range from moments to years. Military examples include grand strategies, strike attack pre-planning, route mission planning, and the acquisition process. Civilian sector examples could include home selection or financial or vacation planning.

Reactive Acts (functions that are an offshoot of the deliberate act). These are actions that were not pre-planned but are opportunities that arise from the moment. In the military, these are commonly referred to as "targets of opportunity." Extending the strike-planning example, consider an Air Force mission to neutralize an airfield: reactive acts would include unscheduled attacks on an unreported new or mobile surface-to-air missile, or on some other unanticipated target of interest, such as an aircraft encountered en route. Timing for these actions is much shorter than for deliberate actions and may range from minutes to hours. Some planning may be involved; however, not all contributing factors are considered, and little time is afforded for risk mitigation.

Defensive Acts (automatic or *conditioned response;* actions that do not require specified premeditated processes). Natural operations that fall into this group include reactions as simple as the eye blink and as complex as tactical air maneuvers. Although the eye blink itself is an instinctive defensive behavior, behavioral psychology has shown that conditioned responses can become as automatic as innate behaviors. Air Force pilots have learned to engage in conditioned responses such as maneuvering or jinking techniques when avoiding anti-aircraft-artillery. Computer users, accustomed to software-induced system freeze-ups, automatically tend to initiate the reboot sequence when their computer fails to respond. Conditioned responses do not afford any consideration of contributing factors or risk mitigation.

"Modern military theory divides war into strategic, operational and tactical levels" (*AFM 1-1, Vol. II*, 1992, p. 43; see insert). Within all levels of warfare there remains some functional

consistency (i.e., planning, and strategy implementation). Therefore, these three distinct OODA Loop modes can also be loosely aligned with strategic and tactical operations.

At the strategic level of war, military and civilian leaders determine crucial priorities between theaters and service efforts, set the focus of military operations, and define the military goals necessary to achieve political objectives. On this level, commanders decide how best to use available resources to achieve larger objectives. Military strategist von Clausewitz is quoted within an Air Force overview on the nature of war on the military leader charged with executing strategy:

> Everything in strategy is very simple, but that does not mean that everything is very easy. Once it has been determined, from the political conditions, what a war is meant to achieve and what it can achieve, it is easy to chart the course. But great strength of character, as well as great lucidity and firmness of mind, is required in order to follow through steadily, to carry out the plan, and not to be thrown off course by thousands of diversions. Take any number of outstanding men, some noted for intellect, others for their acumen, still others for boldness or tenacity of will: not one may possess the combination of qualities needed to make him a greater than average commander.

> On the operational level, military leaders must use their forces to achieve objectives that support the political and strategic goals for which their nation is fighting. Commanders attempt to decide when, where, and under what conditions their forces will attack or defend to support those goals. In the conduct of operations, the enemy presents enormous imponderables, because he is a living, breathing opponent who aims to thwart our every move by maneuvering and acting in accordance with his own designs and purposes, not all of which we may expect. The building blocks utilized in operational plans and execution are the tactics of the forces and the weapon systems of the different services.

> The tactical level of war deals with the basic, fundamental employment of weapons and troops to defeat, kill, and destroy the enemy. Skillful tactical employment is crucial to the conduct of operations. It is on the operational and tactical levels that battlefield success rests. But commanders must recognize that

battlefield success is meaningful only within the larger context of sound strategic and political objectives (*AFM 1-1, Vol. II,* 1992, p. vii).

Very seldom is the decision-making process a single iterative action; rather, it is a composite of several operations, or linked processes, or team interactions. In order to interact with, or to counter, or to affect these processes, it may require several decision attack points or courses of action. Figure 2 shows the linear interaction and the linking of several OODA Loop processes. In reality, the OODA Loop interaction is a non-linear, multi-, or four-dimensional iterative process. This interaction can significantly modify or affect the end result of the proposed plan or action.

Figure 2. Linear OODA Loop Depiction.

Table 1 examines how some effects of this interaction can affect the overall plan.

Table 1. OODA Loop Modes

Type of OODA Process	*Civilian*	*Possible End Results*	*Military*	*Possible End Results*
Deliberate Actions *(Strategic)*	*Take a planned trip.*	*Safe arrival at destination at a predetermined time.*	*Mission planning*	No deviations or changes to plan. Effective mission; all objectives obtained.
Reactive Actions *(Operational)*	*Take an unscheduled exit or detour while driving.*	*Lost time, late arrival; trip not accomplished.*	*Bombing unplanned target of opportunity.*	Primary target not destroyed; loss of time.
Defensive or Conditioned Responses *(Tactical)*	*Swerve to miss a deer or pot-hole.*	*Increased stress and tension; possible damage. Safely avoided crisis situation.*	*Jinking*	Aircraft saved; loss of fuel; increased stress. Primary objective may not be obtained, or worst case scenario—aircraft lost.

There are several reasons why the decision-making process cannot be defined as a linear process. Multiple actions can be processed during the same timeframe and particular actions may cause the DM process to revert backward, skip forward, or move laterally. In the heat of combat, these multiple DM timelines begin to narrow and blend. For example, Lieutenant Colonel Glenn

Larsen, an Air Force tactical reconnaissance pilot, provides the following real world example of timelines blending. Col Larsen recounts an instance during an operational readiness exercise mission where his objective (i.e., the focus of his deliberate action) was to obtain photographic coverage of a recently attacked target. Nearing his goal, and with only 10 seconds remaining to "time over target," Col Larsen was engaged by an aggressor aircraft. His immediate response was to maneuver defensively (his conditioned response) in order to evade the air threat. But, at the same time, he remained focused on the initial objective—getting photographic coverage of his target. So, in the process of evading the aggressor, he maneuvered his aircraft back to the target for the photos (his reactive response) and successfully completed his mission. Had he successfully evaded the air threat, yet returned without the target photos, his mission would have been a failure. His actions combined both reactive actions and conditioned responses in order to maintain situational awareness and complete the mission. See Figure 3 for a breakdown of activities.

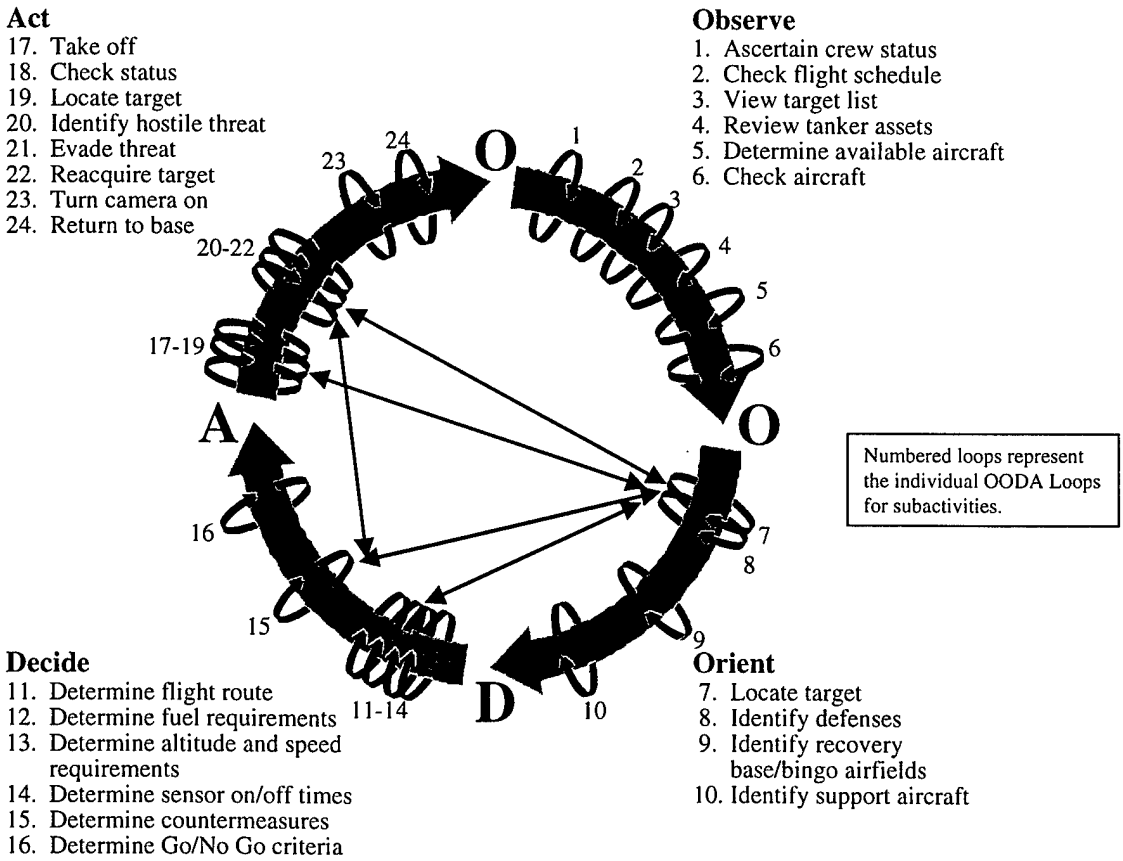


Figure 3. Multiple OODA Loop Interactions.

Deliberate actions may interact with various reactive or defensive acts shown in Figure 3. In this drawing, the deliberate act was to plan and execute a reconnaissance mission. Each deliberate, reactive, or defensive action represents a unique individual OODA Loop action required to conduct the mission (note that this represents only a fraction of the actual iterations occuring during a real mission and may not depict actual order of events). Defensive actions taken in steps 20-22 could have been catastrophic for the successful completion of the mission.

The major factors influencing the OODA Loop actions are time, environment, and level of risk. Figure 4 shows that as time decreases, the OODA Loop becomes a more reactive or more defensive process, and fewer outside factors are considered.

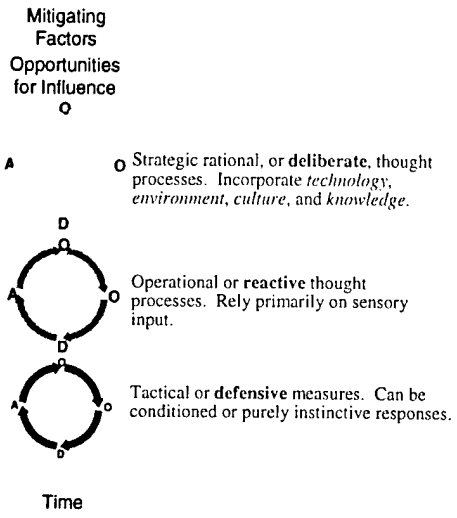


Figure 4. OODA Loop Influences.

Deliberate, *reactive*, and *defensive* acts (DRDA), in addition to defining users actions, may help define an individual's role, thereby providing a means for exploitation of the OODA Loop process. Within each organization or team, different roles may be purely reactive or deliberate. The roles of aircrews, air traffic controllers, and ground fire support teams easily span the spectrum of DRDA. For instance, a fuel truck operator role may have a deliberate function within the squadron. However, the individual's role is purely reactive (i.e., he fuels the aircraft with a specified amount of fuel only when tasked to do so). Similarly, intelligence analysts tend to operate in the reactive mode. There may be collection and mission plans, and long-term

objectives, but for the majority of the time, the analysts are responding to stimuli in a purely reactive mode. Imagery or signals are received, and the analysts respond to the stimuli and interpret the data. Patriot missile crews have both a deliberate and a reactive mode, but the majority of operations are conducted while engaged in the defensive mode.

The OODA model provides a simplistic picture of the major decision-making processes for an individual action or for a planning cycle. However, meeting the ever increasing demands to model or predict the reactions of adversaries requires a more in-depth understanding of the underlying processes involved. Essential to analysis of the decision-making process is an understanding of perception. Perception can be defined as the detection and interpretation of sensory stimuli. The sensory system collects data from its sensors and transfers them to the system's interpretive center, the brain. For each individual, the initial perceptual experience in the brain is mediated by technology, and interpretation is further influenced by the interaction of such personal constructs as emotion, culture, faith or beliefs, knowledge, and intuition. For example, emotion plays a vital role in warfare. "War is a human enterprise. The use of violence injects levels of emotion and ferocity into war that tend to undermine the rationality and cloud the vision of friend and foe" (*AFM 1-1, Vol. I*, 1992, p. 1). Dr. Antonio Damasio, in his book *Descartes' Error,* writes "emotions and feelings may not be intruders in the bastion of reason at all: they may be enmeshed in its networks, for worse *and* for better" (1994). The emotional experience of intense rage can deter "rational" thought processes. Loss of family members or friends can provoke an individual to lose control and lash out against the perceived instigator, without considering the consequences.

The above-mentioned personal constructs comprise a set of "core" elements that, as such, provide a significant influence on the battlefield; they must be considered in the planning process. The modeling of the complexity of warfare can range from difficult to overwhelming, especially when it comes to recreating the infamous "fog of war." "Uncertainty, or the fog of war, constitutes one of the most serious sources of friction in war by making things appear entirely different from what one had expected" (*AFM 1-1, Vol. II*, 1992, p. 18). We understand that each individual will perform the functions captured by the OODA Loop, but not always with the same intensity nor with the same results. A more in-depth look into the OODA Loop model is required in order to examine the key factors that influence the differences in intensity and in results. The personal constructs of emotion, culture, faith or beliefs, knowledge, and intuition, as well as the

differing influences of technology, all mediate our individual perception of events. This personal perception is the most critical element of the decision-making process.

Perception is influenced by the unique elements that make us individuals. Those elements include access to and experience with available technology, emotional makeup and emotional responses (including trust and will), culture and cultural interactions (as well as cultural aspects such as beliefs, both religious and secular), and forms of knowledge (such as education and training), etc. All of these factors play a significant role in developing perceptions. They both can and will cause different responses within each individual or group. In order to study the influence of perception on the OODA Loop, the Technology, Emotion, Culture, and Knowledge (TECK) model has been created. These constructs have been selected as representative of the types of psychologically based influences which contribute to and modify the activity of the core DM element, perception. The TECK model is shown in Figure 5. The model shows that both the perception-based external operational environment and the internal influences on perception affect the OODA Loop. Within the OODA Loop, the core responds to a stimulus event, or sensory input. The stimulus is generated from the external environment. The stimulus creates a sensory input in the form of either information or data. Each of the TECK elements is influenced by and reacts to the stimulus. The reaction contributes to the formation of an interpretation or perception of the information inherent in a given stimulus. The TECK model comprises four elements that may be defined as follows:

> **Technology**—Comprises both rudimentary and complex tools, including electronic equipment (both hardware and software), and all types and forms of communication devices (electronic and otherwise).
>
> **Emotion**—Covers the entire range of our concepts of emotion (love to rage), stress, attitude, trust, and will.
>
> **Culture**—Includes economical, political, and social interactions and our concepts of the rules that govern them, individually held beliefs, faith, and religion.
>
> **Knowledge**—Concerns skills, formal or informal training, experience, rules, laws, standard operating procedures (SOPs) or rules of engagement (ROEs).

For each activity within the OODA Loop, a unique interaction occurs between the TECK elements and the received stimulus. As the received stimulus is transmitted throughout the brain (or, in an organizational analogy, as it is transmitted throughout the organization) each element

helps mold the interpretation of the data presented. The interaction among received stimuli, TECK elements, and the perception/final interpretation form the "lanes of decision," or pathways, that quarter the OODA Loop.

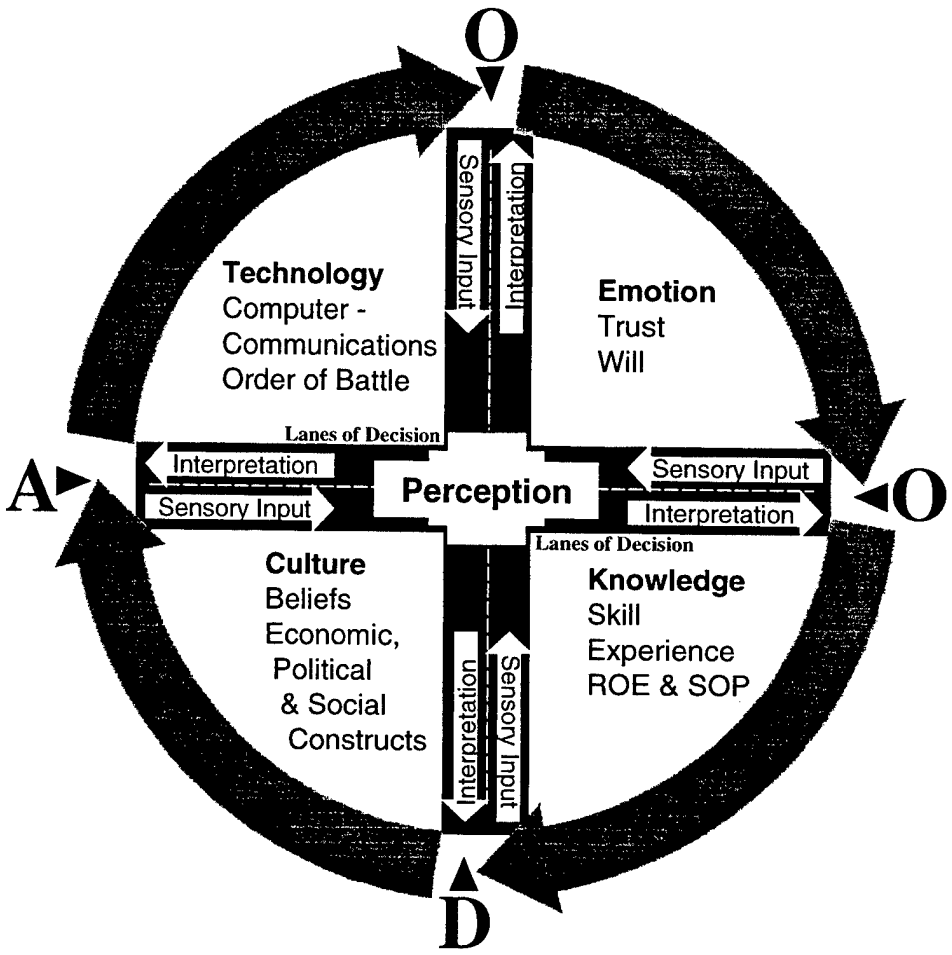


Figure 5. The TECK Model.

A detailed example of how the four OODA Loop activities can influence an individual or organization is provided by examining the actions of an imagery analyst (IA). Photographic interpretation is a basic analytical skill within the military intelligence field. Transforming the "data" provided in imagery into "information" is a complex problem. As previously stated, the analyst's operations tend to be performed in the reactive decision-making mode. Typically, the analyst's first task is to receive the imagery and view/scan the imagery, searching for areas of interest, or "highlights" (*Observe phase*). The analyst orients the image in multiple ways, trying a geographically based (North orientation) or coordinate-based (latitude/longitude) sensor or

perspective view (*Orient phase*). The analyst then determines the information contained within the image (*Decide phase*). Finally, the analyst creates and submits a report of the findings (*Act phase*). The operations are easy to model, being relatively simple and repetitive, and they fit the basic OODA Loop nicely. But what do we find when we explore how the analyst is influenced by the TECK core?

The following story, based on an actual event, illustrates the complexity of the modeling problem. A relatively inexperienced, but "professionally" trained, analyst was reviewing numerous frames of imagery. For one particular image, the analyst's sensory input was degraded (i.e., the stimulus was poor quality imagery). The analyst was forced to rely heavily on the TECK elements for his interpretation and focused on his acquired knowledge of previous intelligence and technical reports. The reports identified the target of interest as a known military training exercise area. This training area was normally used to provide maneuver training for armored tank unit personnel prior to their actual deployment. The analyst's belief system was thus salted with a preconceived expectation of signs of tank activity, which led him to alter his thought process accordingly. Within the image, the analyst observed over twenty large objects that he believed to be tanks. In imagery of the area two days prior there were no such objects reported. The analyst's logic, influenced by his preconceptions, led him to entertain the notion that he was looking at training activity. Lack of experience impeded his exploration of other possibilities, and therefore, impaired his ability to explain the unusual heightened activity. The analyst's interpretation identified possible significant exercise activity (often the precursor to a major deployment), a phenomenon that could lead to major operations, including incursions by hostile forces. He produced a message reporting the heightened activity. The analyst's SOPs required peer review of reports of significant activity. A more experienced imagery analyst/reviewer reviewed the "highlight" message. The reviewer, who was raised in a rural community, informed the junior analyst that it was harvest time (based on the plow rows visible in the field) and that his significant tank exercise activity was nothing but a series of large bales of hay.

This event illustrates how the OODA Loop activity nodes, influenced by the TECK elements, can affect both an individual decision-maker and an organization. However, it also illustrates the shortcomings of conducting performance analysis (or predicting performance effectiveness) using only the basic OODA Loop model. Within the limited framework of the OODA Loop model, the first analyst's assessment was thorough and complete. The analyst

1) observed activity in the imagery, 2) oriented the image with regard to location and historical activity, 3) decided how to characterize ongoing activity and how to determine the appropriate response, and 4) acted to prepare a report. This cycle constitutes a complete OODA Loop; nevertheless, the wrong conclusions were extrapolated! Clearly, a reassessment of the use of the OODA Loop is called for.

Decision-making actions, whether deliberate, reactive or defensive in nature, are all based on the TECK composition. Each situation and each stimulus has the potential to produce a different result or perception. Since perceptions are the primary target of information operations, knowing the adversary's thought processes (and possible reactions) is critical to the successful implementation of an IO attack. Jervis, Lebow, and Stein (1985) state that "perceptions are strongly colored by our beliefs about how the world works and what patterns it is likely to present us with." Therefore, the decision-maker who thinks that the object of interest is the product of a hostile adversary, will interpret ambiguous information as confirming his image; whereas, the same information about a country thought to be friendly would be construed to offer no threat. This coloring of perception forces the careful decision-maker to delay action, reassess each situation, and only then, react to his perception.

Franklin C. Spinney, a Pentagon defense analyst and colleague of Col John Boyd, has written a number of papers on the use of the OODA Loop in modeling modern warfare activities. He has analyzed the OODA Loop itself and in his presentation, *Evolutionary Epistemology*, a discourse on Boyd's *Destruction and Creation*, he states that, "All observations of the external world are filtered through the cognitive apparatus of the observer... And therefore...observations should not be separated from the various interior mental processes of each observer" (Spinney, 1997, p. 3). The individual's multiple perspectives, based on his personal mental concepts filter his experience. He sees the "observing apparatus" as an evolutionary force that both shapes and is shaped by the object under observation and "the interaction of environmental pressures" (1997, p. 13). In his detail of the Orientation phase of the OODA Loop, shown in Figure 6, Spinney points out that orientation shapes observation and decision, and is influenced by the feedback and other phenomena that enter our consciousness through observation—*orientation* is the heart of the OODA Loop cycle (1997). Within the orientation activity, he identifies genetic heritage, experiences, and cultural traditions as moderating influences.

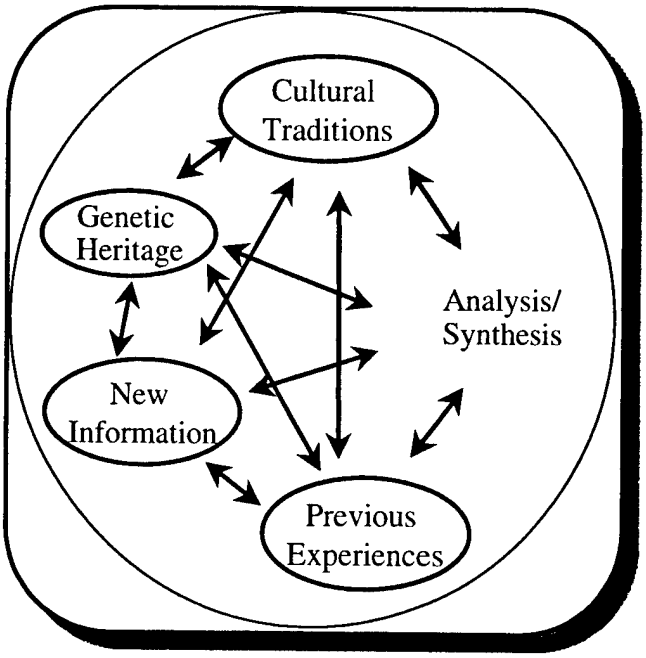


Figure 6. Detail of the OODA Loop Sketch: Orientation (Spinney, 1997).

Cultural traditions are clearly an important component of our decision-making process. Cross-cultural differences often cause different reactions. In observing and studying international conflict, "it becomes apparent that the participants almost never have a good understanding of each other's perspective, goals, or specific actions. Signals that seem clear to the sender are missed or misinterpreted by the receiver; actions meant to convey one impression often leave quite a different one" (Jervis et al., 1985).

The conduct of a celebrated U.S. hostage crisis vs. an alleged Russian solution provides a study in cultural contrasts and how they affect both situation assessment and response. On Nov. 4, 1979, 52 of the 90 employees of the U. S. Embassy staff in Iran were taken hostage by Iranian revolutionary terrorists. President Jimmy Carter applied economic pressure, ending Iranian oil imports and freezing almost $8 billion in U.S.-held Iranian assets. He also initiated a number of unsuccessful diplomatic efforts to free the hostages. An attempted military operation failed, as well, and Carter's reelection loss to Ronald Reagan is attributed (at least in part) to a continued failure to resolve the hostage crisis. In January of 1981, following Iraq's 1980 invasion of Iran (a probable distractor) and mediation by Algerian diplomats, the Iranians finally released the hostages—444 days after taking them (Sick, 1985).

Allegedly, Russian KGB agents were faced with a similar situation during the same timeframe. In the version of a story which circulated throughout the U.S. military community, KGB agents simply kidnapped the Iranian terrorist's family members and began to mail body parts back to the terrorist, beginning with fingers. According to the story, this action prompted the terrorist to release the Russian hostages immediately. In both cases the countries sought the same resolution; however, judging from the results, the Russians applied a better "cultural" understanding of the terrorist's mindset and responded "in kind" to the terrorist act. The U.S.' emotional, moral, and cultural constructs would prohibit policymakers from employing similar tactics. This example, even if only partially true, illustrates how cultural constructs such as principles and ethics (elements within TECK), including the constraints imposed by one's own culture, are factors that must be considered when dealing with an adversary.

In order to predict the adversary's decision-making actions, a complete understanding of the adversary's principal TECK influences is required. Operational planners and decision-makers must fully understand the motive forces that drive an adversary's actions. "It is generally easier to induce an enemy to maintain a pre-existing belief. Thus, it may be more useful to examine how an enemy's existing beliefs can be turned to advantage than to attempt to change his beliefs" (FM 90-2). Using predictive analysis, once the adversary's TECK core is understood, it can then be exploited through perception management to elicit the desired response, or to force the adversary down pre-identified decision-making paths.

Perception management is defined as those "[a]ctions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning; and to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover and deception, and psychological operations" (*Joint Pub 1-02*, 1999). Once initiated, if an adversarial force is neither swayed nor deterred, nor influenced by information operations, the initiator has gained nothing.

One of the most cunning information operations in perception management (and in prediction analysis) ever conducted was the "Man With No Name" (or "Operation Mincemeat") deception of World War II. This grandiose British ruse was an attempt to convince the Germans

that the main thrust of attack in the push for Southern Europe was to begin jointly in Sardinia and Greece. The British knew the Germans would not accept any information provided by a fortuitous major British security violation (e.g., spies, conveniently "lost" documents or easily intercepted voice communications). To accomplish their mission, the British would have to provide the information by means plausible to the Germans.

The British opted to exploit the non-official relationship between Spain and Germany. They invented an officer, Major Martin, in 1943. Major Martin was reportedly a courier for the British High Command. The ruse was designed to place in German hands documents that contained only preliminary indications of the attack. The information was inserted in private letters of the General Staff, London, and Field Marshal Alexander in Tunisia. The plot was simple: to supply the Spanish with a dead man, carrying secret communiqués referring vaguely to troop movements and to let the Spanish government transmit the supposed "plans" to the Germans.

The details of the operation were excruciating. The British used the frozen body of a recently deceased man who had died of pneumonia (the family wanted his name never to be revealed, hence the title, "Man With No Name"). Secret reports of a missing courier were generated, as was evidence suggesting a fake fiancée. Theater and club tickets, personal letters, overdraft statements, etc., were all produced and planted on the body. The Spanish found the body washed ashore, and did, in fact, turn the information and body over to the Germans. The Germans investigated every detail completely and thoroughly before they allowed themselves to be convinced of the validity of the communications (Dulles, 1968).

The entire operation would have been for naught if the body was never found, if the Spanish did not turn over the body to the Germans, or if the planted secret information contained too many or too few details to be plausible. The operation dealt entirely with the manipulation of the adversaries' perceptions in order to influence multiple operatives/decision-makers' decisions.

In addition to predictive analysis, post TECK analysis is required to plan effectively for future IO endeavors and to ensure a successful information warfare campaign. This new form of predictive analysis can be considered an enhanced IPB for IW operations. Advanced technology is not always the best answer. Take, for example, that country "X" is engaged in hostile activity against the U.S. military. One effective IO tool that might be applied against the U.S. is denial of

electrical service. The loss of all electrical power would have a severe impact on the U.S. and would conceivably have a similarly negative effect on an adversary. Its potential impact was demonstrated in Maine and Canada during the winter of 1997, when ice storms left the northern state and Canada without power for weeks, and again in Virginia in January, 1998, when heavy storms denied power to thousands of inhabitants for over a month. Loss of simple functions like the ability to heat homes, pump gasoline, and shop for groceries crippled the public. Many normal day-to-day operations ceased—inhabitants endured limited radio service, no television or telephones, and loss of most computing systems—causing mass disruption to the information infrastructure.

During military operations, similar attacks or effects could be duplicated with either standard munitions or offensive IO tools. This tactic, depending on the adversary, might or might not have a significant impact on the adversary's OODA Loop. For instance, Third World countries, whose utilities often do not provide continuous daily service, may suffer from frequent power shortages, and the people are accustomed to living within the constraints such interruptions in service impose and plan for them. Conceivably, they might not be as adversely affected as U.S. citizens or the citizens of any other industrialized nation. Most military systems would not be immediately affected due to the possession of power generator backups.

Similarly, if complex IO measures were employed against an adversary that was either unaware or undaunted by the operation, the attack would fail and potential benefits from the operation would be lost. Thus, Sun Tzu's adage, "Know thy enemy...." (1963, p.84) is particularly appropriate to the effective use of IO. Applying the TECK model within the IO framework, there are numerous methods and techniques strategic and operational commanders can employ to elicit desired reactions. Some of these methods are discussed in the following chapter.

METHODOLOGIES FOR ALTERING OR INFLUENCING THE DECISION-MAKING PROCESS

Altering or influencing an adversary's integral decision-making process is the ultimate goal of the IW attack. Within IW, IO focuses on attempts to confuse, misguide, overload, or delay the decision-makers' thought processes. Decision-makers acting on false or incorrect data are more likely to make a final decision that is some degree askew from an accurate or appropriate decision (see Figure 7). This provides a "soft kill" vs. a "hard kill" solution. One renders the enemy defenses ineffective and may even tie up forces or resources not directly targeted, while the other destroys them, often with unavoidable and not necessarily desired collateral damage. IO includes indirect methods of attack—military deception and psychological operations, as well as the direct information attack. Direct attack alters the content of information, while leaving it apparently unchanged. Indirect methods, however, involve perception management and management of the decision processes of those who use the information. Indirect attack methodologies and an analysis of information operations opportunities and issues are offered on the following pages.

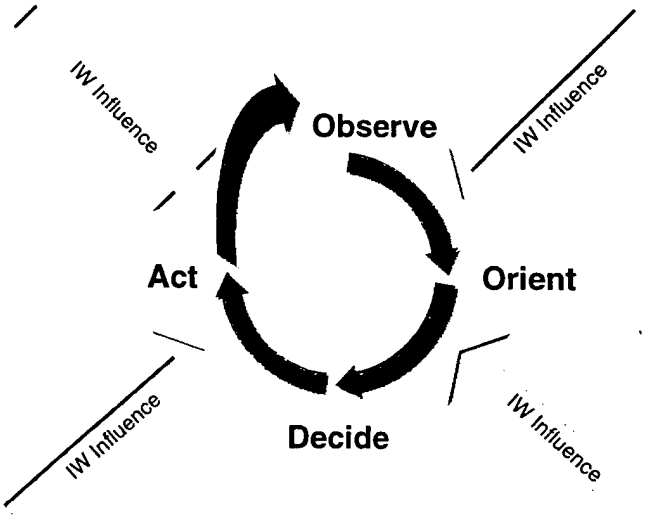


Figure 7. The OODA Loop Set Askew.

Military Deception is defined as those "[a]ctions executed to deliberately mislead adversary military decision-makers as to friendly military capabilities, intentions and operations,

thereby causing the adversary to take specific actions that will contribute to the accomplishment of the friendly mission" (*Joint Pub 1-02,* 1999). One of the first survival tactics developed by mankind was the active application of Camouflage, Concealment, and Deception (CCD) techniques. Now considered a tool of military deception, the role of CCD was critical for survival. It enabled hunters to trap game and to hide from and defeat potential enemies. *Camouflage* is "[t]he use of natural or artificial material on personnel, objects, or tactical positions with the aim of confusing, misleading, or evading the enemy" (*Joint Pub 1-02*, 1999). In nature, it enables the most vulnerable of creatures to remain undetected by its predators. *Concealment* hides critical components and denies access to potential targets by protecting them "from [enemy] observation or surveillance" (*Joint Pub 1-02*). *Deception* is "[t]hose measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests" (*Joint Pub 1-02*). *Air Force Instruction (AFI) 32-4007* (1994) describes CCD as supporting "Air Force war and contingency plans by minimizing the loss of operational capability during contingencies. The highest priorities are force survivability and mission continuation. CCD refers to the capability to reduce the effectiveness of attacking air and ground forces and reconnaissance assets. CCD includes the principles of hide, blend, disguise, and decoy to protect friendly aim points with materials and equipment to alter or obscure part or all of their multispectral signatures." The Joint Chiefs of Staff emphasize CCD's efficacy in joint operations. "The use of CCD provides JFCs [Joint Force Commanders] with means of portraying the situation they want the adversaries to observe" (Air Land Sea Application Center, no date).

Throughout history CCD has played a significant role in both military victories and defeats. CCD is the secret weapon that empowers military commanders to achieve surprise, promote security, and "seize the initiative, actively misleading the enemy tactical commander" (*AFI 10-704,* 1997). The ultimate CCD application is the Greek tale of the fall of Troy—passed from generation to generation, from the Golden Age of Greece to the present day. The Trojan Horse, a story known by everyone who ever studied Western history, is one of the most dramatic camouflage applications in history. In the *Aeneid*, the Roman poet Virgil tells the story of the Trojan horse, left outside the gates of Troy by the retreating Greeks. A Greek spy posing as a defector, Captain Sinon, told the Trojans that the Greeks had sailed away, leaving the Trojan Horse behind as a tribute to the gods. The Trojans were intrigued and towed the enormous

wooden horse inside the city and began to get drunk, celebrating their victory. That night, inside the ordinarily impassable city walls, a handful of Greek soldiers hidden within the belly of the horse slipped out unnoted by the celebrating Trojans. The Greeks opened the gates to their army, which had only sailed out of sight and had returned under the cover of darkness. The Trojans were in no shape to provide serious resistance and the invading Greeks captured the city of Troy.

Other examples of CCD are woven through our own military history; George Washington reportedly used deception tactics during the Revolutionary War. He strategically lost a saddlebag of fake plans where the British would find them. However, no information operations effort compares with the large-scale activities during World War II. The Japanese, Germans, Russians, British, and Americans all engaged in full-scale information operations. The preparations for nearly every battle incorporated feints, misdirections, secret locations, and camouflage.

The British actively employed several groups of its military intelligence organization to study and develop methods to deceive the Germans. One such deception group operated in North Africa, and it deployed entire battalions of decoy tanks and artillery in efforts to deceive General Rommel's forces. The African group enlisted the aide of a master magician, Jasper Maskelyne. One of his most successful acts of deception and camouflage during the war was hiding the Egyptian port of Alexandria from German bombers. Alexandria was crucial to Allied logistics operations in Africa. "Seen from a bomber cockpit, Alexandria Harbor was an easily distinguishable target" (Fisher, 1983). Maskelyne was tasked with hiding or camouflaging the harbor until fresh troops and supplies could be successfully landed. To do so, Maskelyne used a technique called "substitution" or "transposition." Approximately a mile down the coast from Alexandria lies Maryut Bay; Maryut Bay has a shoreline similar to Alexandria's. Maskelyne created ground lights, structures, fires, defensive positions, and a false naval destroyer so that from the air, Maryut Bay would appear to unsuspecting pilots to be Alexandria. The German pilots conducted their bombing runs over the false port. To sell the success of the bombing runs to the German High Command, Maskelyne seeded Alexandria with rubble and fake or painted bomb craters. During the day, German reconnaissance planes photographed and observed the simulated damage sprinkled throughout the area. After eight nights of apparently successful raids on the artificial port, the Germans ceased the bombing runs—the ruse was considered a success, and the port was spared.

In information operations, illusions are a way of life. Maskelyne was successful because he provided the key elements required to make the illusion work. He manipulated the components of the German pilots' OODA Loops, providing all the perceptual elements that the Germans were anticipating. If the planned ruse was decoy tanks and artillery, Maskelyne supplied smoke, flashes, and sound to sell the deception. All good magicians use the same rule: provide the audience with what they expect to see, and the audience will create its own assumptions.

The great illusionist Harry Houdini was a master of perception manipulation. During his "Chinese Water Torture Chamber Escape," he would ask the audience to take a last breath with him, and then hold its collective breath for as long it could. When no one in the audience could hold his breath any longer, fear would overcome the watchers, who felt sure that, this time, Houdini must have died. After an appropriate period of time, Houdini would appear, gasping for breath—all an illusion. These techniques are baseline for CCD operations; they provide the audience (or adversary) a plausible solution and allow the adversary to draw its own conclusions and alter its chosen course of action accordingly.

A course of action (COA) is "[a] plan that would accomplish, or is related to, the accomplishment of a mission" (*Joint Pub 1-02*, 1999). The COA is merely a compilation of possible OODA Loop responses, and as such, is vulnerable to attack. In order to modify the adversary's thought processes or to redirect the adversary's focus, any number of CCD or IO applications may be applied. The business and time management professional, Steven Covey, provides a quote that is very apt when applied to information operations: "[B]egin with the end in mind" (1990).

Normally, deception is applied when one wants to elicit a particular reaction from an adversary. In the deception flow model depicted in Figure 8, a deception technique or stimulus such as a decoy is employed. Once deployed, the decoy is either observed or not. The intelligence filter (this is not solely an "Intelligence Organization" function; it could be whoever detects the activity) provides the first attempt to interpret the data. The filter then supplies a personally biased interpretation to the decision-maker. In deception operations, the decoy is targeted to influence the decision-maker, not necessarily the intelligence filter. After receiving the information, there are at least three possible COAs the decision-maker may choose:

- A *positive* reaction—the decision-maker reacts to the decoy by either attacking or maneuvering in direct response to the decoy, as intended
- A *negative* action—the action of the decision-maker is directly contrary to the intent of the deception
- *No reaction* to the deception—the decision-maker fails to commit any action

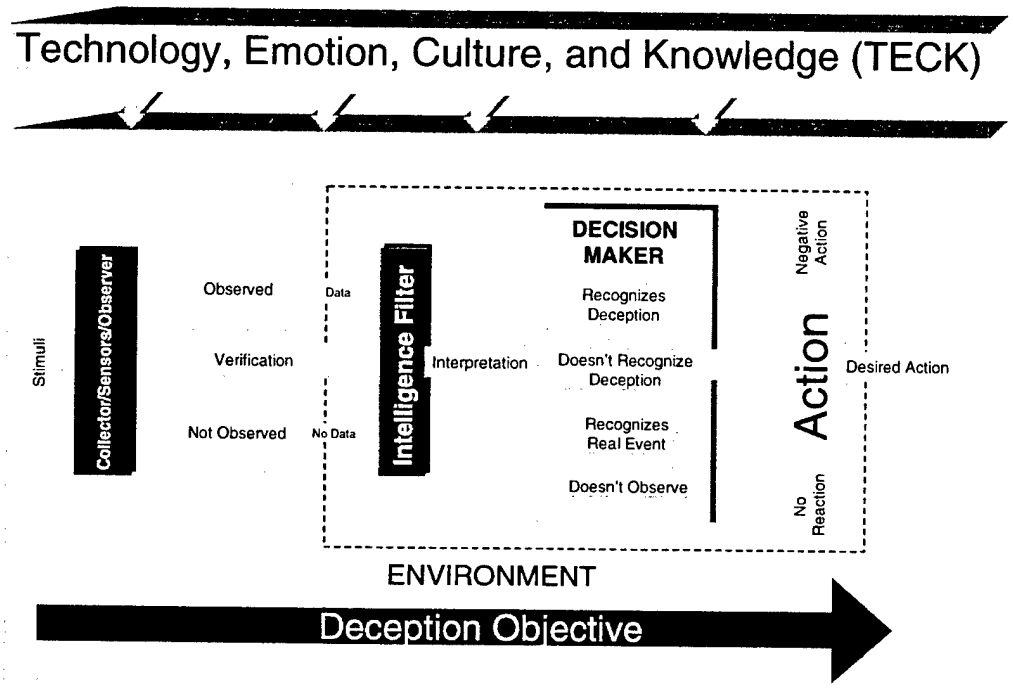


Figure 8. Deception Flow Model.

The Deception Flow Model can be used in conjunction with the OODA Loop/TECK Model in order to conduct a predictive analysis of enemy behavior. In the Alexandria Harbor example, the German decision-makers understood the Port of Alexandria's criticality to the Allied forces' resupply efforts. Suppressing Allied resupply activity was the intended outcome of their raids on Alexandria; the decision to strike the port was the COA. Recalling the three modes of activity previously discussed, selection of strike aircraft, principal targets, reconnaissance, and weapon loads were all examples of *deliberate* OODA Loop activities supporting the COA. Attacking targets of opportunity (the surrogate destroyer) and identifying the target area are examples of *reactive* OODA Loop activities. The German pilots' use of jinking (for flak avoidance) during the bombing runs is an example of a *defensive* activity (an unplanned or unanticipated response). Although the initial decision to bomb the port of Alexandria was an unavoidable German strategic decision, the Allies' creative use of CCD techniques for perception

management distorted the enemy's decision-making process and influenced the enemy's conduct so as to minimize adverse effects—the desired outcome of enemy OODA Loop activity control.

Altering any of the key components of the OODA process prevents the adversary's drawing correct conclusions or making proper judgements. Administered properly, CCD and other perception management techniques can "box in" the adversary. The more reactive *defensive* OODA Loop activities are induced, the more *offensive* warfare capability is decreased (e.g., in chess, opponents' offensive options are significantly reduced while they are responding to check). Maskelyne used the Germans' assumptions about the tactical situation against them; preying upon human error, timing, and the German pilots' continued inability to orient themselves over the target. In order to fully sell the illusion, he supplied the photo interpreters with imagery showing false targets and false destruction, further confusing the German decision-makers. Viewed after the fact, the analysis and its outcomes seem inevitable. However, in any predictive analysis, care must be taken to determine exactly which OODA Loop activities are targeted, the activities' inter-relationships, and the timing of the targeting.

One IO application is deception, whose goal is target or element survival. The "grand ruse" was one of an array of deception and camouflage techniques used to support the Normandy invasion in "Operation Overlord." Overlord consisted of two distinct phases—"Bodyguard" for the strategic deceptions, and "Fortitude" for tactical operations—"mislead[ing] the enemy when preparations could no longer be entirely concealed as to the date, strength, and area of attack" (Dulles, 1968). Deliberate OODA Loop activities were targeted with the use of falsified maps and invasion plans, as well as false communications. Attacks on reactive OODA loop activities featured deliberate attacks accompanied by supporting feints, camouflage, and decoys. Defensive OODA Loop activity attacks were retreats or attacks covered by smoke, chaff, sound actuators, etc.

Psychological warfare is another means of indirect attack used in information operations. It is totally focused on influencing perception—"The planned use of propaganda and other psychological actions having the primary purpose of influencing the opinions, emotions, attitudes, and behavior of hostile foreign groups in such a way as to support the achievement of national objectives" (*Joint Pub 1-02*, 1999). Psychological operations (PSYOP) "can counter foreign propaganda that adversely affects the achievement of U.S. objectives" (Goldstein & Findley,

1996). The primary PSYOP methods are radio and television broadcasts, leaflet drops, news management, and crowd manipulation during rallies and protests. One famous PSYOP application was the World War II "Tokyo Rose" broadcast series, attacks directed at the morale of the military forces. PSYOP are designed to help weaken the adversary's resolve. These operations focus on the emotion component of the TECK model, through both visual and audio messages.

In modern IO, visual and audio systems can be exploited as never before. No longer is data collected solely by human sensory systems. Now, collection systems themselves, as well as their operators, are vulnerable to attack. Traditional IO applications have relied on timing, misinformation, concealment, observation, and opportunity (luck). Cyberspace creates the perfect environment for information operations activity. IO works best when vision is clouded and confusion is apparent. Appearances of plausibility and time constraints add to the situational problem. Uncertainty is inherent in cyberwarfare; operators must rely on bits and bytes to determine their opponent's operational order of battle.

Unlike the operational battlefield, cyberspace prevents traditional reconnaissance—normally, one cannot physically observe actions and reactions. The warfighter conducting information operations encounters a target-rich environment of multiple operational computer systems—the cyberwarfare realm. Now nearly every sophisticated weapon or computer system is at risk. In the past there have been numerous visible and auditory influences to impact the senses (vision—by camouflage, decoys and, smoke and the auditory—by meaconing, jamming, interference, and intrusion). In cyberspace, a totally new dimension is now available with which to attack the decision-makers.

The new threat is the reliability of data. Previously, operators tended to trust the data that they received. For example, the imagery analyst trusted that the image received was actually from the area of interest and that the data accompanying the image was valid. However, a clever cyberwarrior can manipulate the data in such a way that the end-user would not perceive its falsity. A short list of cyber deception methods includes coordinate manipulation (the user or system is looking at a different area than is being reported); target generation or deletion by intruder processor algorithms; imagery alteration to deceive automated target recognition systems; alteration of telephone components to call false numbers (when a 9 is dialed, the phone

actually dials a 7), and injection of false or erroneous databases into host systems. Cyber attacks can, in the most drastic case, cause unreported system-component or whole-system shutdowns.

Perhaps one of the most challenging developments of the information age is that the sheer volume of available information can quickly obscure the critical decision-making information. The abundance of information can either enhance or degrade information operations. Control of critical information is a subset of perception management, and is therefore, a prime target of IO. Frustration and indecision are likely outcomes when critical decision-making information is not readily available to an operator. An individual tasked to operate in a degraded information environment can become hamstrung and may resort to guessing rather than providing accurate intelligence. Additionally, "sophisticated presentations can also obscure vital information and/or mask poor quality or incomplete data." (Alberts, 1996). "Uncertainty regarding the quality of the information being presented or its integrity could lead to a lack of confidence that inhibits the use of information or intelligence systems. Decision-makers clearly need confidence in the reliability, currency, and accuracy of data in order to act on it. In the information age, the integrity and authenticity of the data are important" (Alberts, 1996).

As information sources proliferate, individuals receive inputs from multiple sources in a chaotic manner. This asynchronous arrival of information has been found to confuse and distract decision-makers. In response to this phenomenon, numerous efforts are being made to augment the decision-making process with automation or data fusion. One such decision aid, the automated target recognizer, reviews imagery data as it is processed and identifies potential targets. Future IO can be anticipated to target automated target recognizers, modifying the crucial algorithmic backbones of the systems.

Timeliness will become even more critical in future IO. The insertion of timing delays can significantly alter the battlefield. The expectation of near perfect information and the willingness to delay decisions in the expectation of better information will grow. The commander who waits for near perfect information will be defeated by one who acts on "good enough" information.

Exploring the techniques of information operations, we can determine which OODA Loop activities/TECK elements to target and identify methods to optimize the attack. The majority of information operations are designed to reduce the sensory input, or to impact technology.

Looking back at the four components of the combined OODA Loop/TECK model, it appears the primary area of IO attack is the technology sector. Information operations specifically look at limiting the sensory input provided for the adversary's technology. The two primary sensory inputs are the visual and auditory systems; the tools and techniques of perception management target them specifically and provide different effects.

During the later stages of World War II, the British became adept at deception activity. According to the *Army Times*, during Operation Overlord there were seven means for the Germans to acquire intelligence.

- *Luftwaffe* reconnaissance
- Plotting of Allied signal traffic by radio
- Questioning of Allied POWs and members of resistance movements in Europe
- Reports from German diplomats and spies in Eire and other neutral countries
- "Leaks" and careless talk by neutral diplomats in London
- German agents operating in Britain
- Reconnaissance landings by German commandos on British shores

(excerpted from *Great True Spy Stories*; Dulles, 1968)

The British neutralized the majority of the intelligence threats (including the agent and spy networks). They then exploited the others. For instance, they exploited reconnaissance aircraft by allowing the aircraft to fly over prepared deception sites. However, the primary source for deception activity became signal and message exploitation, permitting the British to successfully manage the Germans' sensory inputs.

The sensory inputs can be affected in numerous ways, the following examples elucidate some techniques to alter decision-making.

Camouflage techniques are becoming more advanced each year. Camouflage includes netting, pattern disruption material, and paint schemes that hide personnel and equipment. Initially, camouflage was used to deceive only the visual sensors, including the unaided or augmented eye (eye plus binoculars), and photographic equipment. However, advances in material and paint production enable camouflage techniques to disrupt other sensors, such as infrared or near infrared hyperspectral systems and radar.

Radar systems can be attacked, or easily deceived, using radar reflectors, radar decoys, radar-dampening material like the covering on stealth aircraft, or by using such target confusion techniques as covering tank tracks and removing or adding protruding equipment.

Concealment achieves many of the same purposes as camouflage, but at a much lower sophistication level and a reduced technical cost. However, it hampers mobility and decreases reaction time, which impacts operational flexibility. Smoke does offer a significant advantage against optical systems in tactical or reactive situations, but smoke is only an effective cover for a short period of time, depending on dispersal techniques and wind velocity.

Electronic signal measures are designed to limit the auditory senses or sensors. Signals Intelligence (SIGINT) is one of the most critical intelligence sources available on today's battlefield; it therefore becomes a primary target of IO. Tapes of troop movements, pilot chatter, sounds of tank engines, and naval carrier operations can easily be duplicated (or emulated) and then transmitted through appropriate media, to simulate actual operations. Radar or signal generators can be jammed or flooded and emission control techniques (turning off sensors) can substantially alter the battlefield composition.

The information operations field is evolving at a rapid pace. New sensors (including radar, electro-optical [EO], infrared [IR], multispectral, and acoustic) have increased ranges and cover a broader collection spectrum. Enhanced processors and processing techniques extract even miniscule details. Large volume, rapid retrieval databases; dynamic communications; and faster computers are being developed and fielded. Each of these new developments requires the development of new IO techniques. Simple IO techniques, methods such as applying smoke screens, have been raised to scientific arts. Smoke can now be augmented with particulates, heat generators, and noise generators to misdirect multispectral and other dynamic sensors. Not all sensor reduction techniques and schemes are expensive or elaborate. Measures such as burning tires, lighting numerous fires (e.g., the torching of the oil fields during DESERT STORM) may provide enough of a visual distracter to impact sophisticated sensors and/or delay operations. Loud speaker interference or vibration may affect SIGINT collection. However, the real key to successful employment of IO techniques is to know the adversaries, their capabilities, and their culture.

IW MODELING AND PLANNING TOOLS

Current military modeling applications of information operations do not meet the dynamic challenges of future information warfare. Without proper planning, information warfare is as useful in modern warfare as an unloaded weapon in a hostile firefight, yet IW/IO planning and modeling tools are nearly non-existent. Today's models can accurately portray an adversary's equipment or techniques, but few (if any) models can actually capture the decision-making process.

The dynamics of military operational strategic and tactical planning and execution are analogous to the dynamics of corporate planning. Within the corporate environment, strategic planning is a critical component of the operational process. Strategic planning evolutions are also crucial for the success of information warfare operations. Issues of tool modernization, new plant development, workforce right-sizing, information flow and networking, and union dispute mediation are as difficult as the most complex IW problem.

During the last twenty years, the corporate domain has actively sought solutions to these and other problems. Investigations have yielded insights into the structure, mechanisms and functions of organizations in dynamic environments and of organizational communications, organizational development, and change management. Similar insights have been identified for group dynamics, group vs. individual decision-making, and team formation and function. Disciplines which have risen from these investigations provide paradigms in strategic and tactical operational planning which are equally applicable to the military domain and yield analytical modeling, process evaluation, and process engineering tools which may be successfully used by IW planners. Many such tools are already in use by military planners in organizational management of enterprise applications, but not, for the most part, in operational force application activities.

Process improvement is a blanket term for the disciplines that have sprung from corporate research on organization function and management. Organization Development (OD), Total Quality Management (TQM), and Business Process Reengineering (BPR) all evaluate management of complex, dynamic corporate functions and relationships. Process improvement is a process-focused approach to improve business function, and centers on the mode of production

(of any product), rather than on the product itself. Process-focused approaches may use any systematic technique to identify and analyze problems, evaluate data, and generate solutions. Modeling and metrics are critical elements of process improvement. Modeling tools may be considered organizational intervention techniques, as they permit the analyst to map and evaluate the process prior to altering it and to examine revised processes before implementing them.

Like the other services, the Air Force has embraced process improvement to manage its organizational evolution and has co-opted several constructs to aid planners. The first is the Shewhart Cycle which, like the OODA Loop, is a four-step decision-making model. The Shewhart Cycle, shown in Figure 9, however, is based on the organizational rather than operational environment, and includes the following activities.

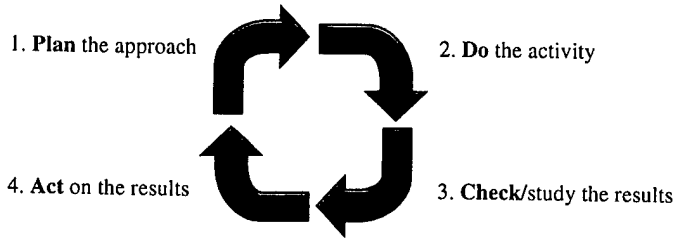


Figure 9. The Shewhart Cycle.

The Continuous Improvement Process (CIP), shown in Figure 10, is an iterative, seven-step process that expands the Shewhart construct, adding more specificity. Both constructs have been adopted to provide a common methodology to implement and manage a process-focused approach.

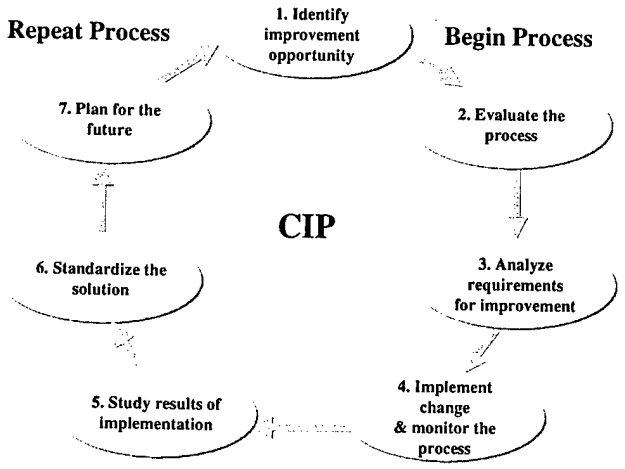


Figure 10. The Continuous Improvement Process (adapted from Holmes, 1994).

Process improvement, and the evaluative disciplines of OD, TQM, and BPR, use modeling extensively. The process improvement task can be divided into six stages which roughly correspond to the steps listed above. Different modeling tools are considered effective at each stage and are listed in the table below. Although the Air Force uses TQM and BPR concepts extensively in their original roles, the tools of process improvement have yet to be applied to operational analysis problems. However, operational decision-makers can also use organization intervention tools to model processes, both for visualization and for analysis.

Table 2. Modeling Tools (adapted from Holmes, 1994)

1. Identify Problem	2. Evaluate Process	3. Analyze Data	4. Implement Change	5. Study Data	6. Plan Future
Brainstorming					
			Force Field Analysis		
Flow Chart	Flow Chart				Flow Chart
		Fishbone			
	Pareto	Pareto		Pareto	
	Check Sheet			Check Sheet	
	Histogram			Histogram	
		Scatter Chart			
Run Chart	Run Chart			Run Chart	
Control Chart	Control Chart			Control Chart	Control Chart

Note: The Standardize Solution step has no charts associated with it.

The premise of organizational intervention is "a planned, systematic process in which applied behavior science principles and practices are introduced into ongoing organizations toward the goal of increasing individual and organizational effectiveness" (French & Bell, 1995). The principles of organization development, although differing in phase divisions and in scope because of the character of the environment in which they are used, are still analogous to intelligence analysis, or operational planning, in which the goal is to analyze the situation, take action or make recommendations, and reanalyze. Analysis of a corporation involves evaluating four primary categories: machine, methods, materials, and man. As with foreign adversaries, corporations have their own TECK core elements. Understanding the corporate core elements and their interactions in OD analysis is as vital as understanding an adversary's potential actions.

As earlier described, the OODA Loop is the prominent model for depicting the integration of IW operations. The OODA Loop provides a high level definition of operational thought processes and enables them to be mapped for creative exploitation. However, the OODA Loop is not sophisticated enough to model the intricate planning evolutions of IW activity, specifically the various technological, emotional, cultural, and knowledge-based influences. However, there are several intervention tools (such as force-field analysis, cause and effect, and process flow diagrams) that illuminate different facets of the IW processes and provide equally valuable methods for mapping complex IW operations.

For successful planning operations, it is imperative to map the adversary's perception and potential reactions. In other words, determining "what buttons to push" to elicit a desired reaction is crucial. Another Steven Covey quip applies, "Seek first to understand, then to be understood" (1990). The elements that need to be monitored and eventually managed are *cause* and *effect.* The disciplines of Business Process Reengineering and Total Quality Management have dealt with functions through force field and cause and effect analysis for years. Dr. W. E. Deming led the development and implementation of many process evaluation tools and integrated others into his Total Quality Management methodology. Several tools, force-field analysis, Ishikawa "fishbone" diagrams, and run charts will be discussed.

Force-field (or vector) analysis is used in organization development to plan actions to bring about specific changes. In force-field analysis, the current situation is evaluated and a future goal identified. Measures are placed on either side of a vertical line representing equilibrium. The measures constitute the driving or restraining forces which may counterbalance one another. The intent is to sufficiently weight the driving influences such that they outweigh the restraining forces and move the equilibrium horizontally to the desired goal (see Figure 11).

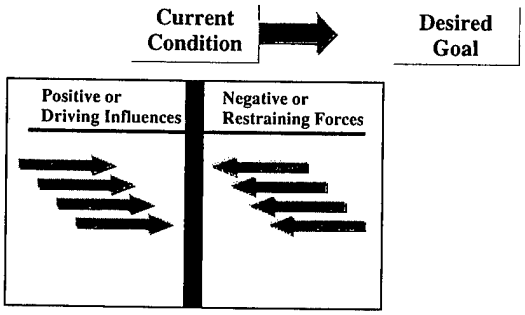


Figure 11. Force Field Analysis.

Another tool that Dr Deming adopted is known as the Ishikawa diagram, commonly known as the "fishbone," which was developed by Kaoru Ishikawa (Clemson University, 1997). The fishbone diagram provides a graphical representation of problem causes and/or key factors that may lead to success; its use is also called cause and effect analysis. Fishbone diagrams are used to explore materials, man, machine, and methods. Typically, fishbone diagrams have at least four major influences; if necessary, others can be added. These diagrams resemble the bone structure of a fish (see Figure 12).

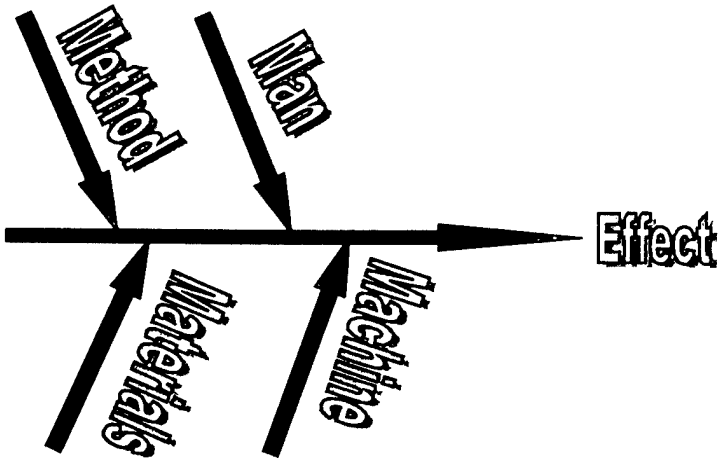


Figure 12. Ishikawa "Fishbone" or Cause and Effect Diagram.

In addition to the main spines, subcategories, or more specific details of causes, can be included to complete the entire picture. Besides listing the data on the fishbone, this intervention analyzes the "whys," manipulating the spines to represent critical elements of information or causation.

Considering that not all planning or influence factors are constant or balanced, decision-makers could employ "inertia" analysis as part of the planning process. Inertia analysis can be used to evaluate positive and negative aspects of cause and effect. The fishbone can depict the counter-acting forces with the amount of influence, modeling by line length, width, intensity, or color. Once all the factors are graphed, analysis is conducted to determine which conditions can be modified for the preferred effect.

Figure 13 and Table 3 represent how the fishbone intervention technique can support IW or CCD operations, in either the planning or decomposition stages. The following scenario is based on a sample of operations from the "peacekeeping" operations in Somalia during the mid-1990's and is selected for modeling. General Mohammed Farah Aideed, warlord leader, managed a successful IW campaign against a "superior" and more technologically advanced adversary. In reviewing the historical events of the operations in Somalia (see Table 3), military analysts, using the fishbone model, can extract pertinent elements of IW operations and possibly develop a predictive analysis tool. Figure 13 depicts how some of the events could be modeled, showing the perceived amount of leverage and the opposing forces applied. Similarly, this model could be invoked for predictive analysis by assessing each opposing force and plausible reactions.

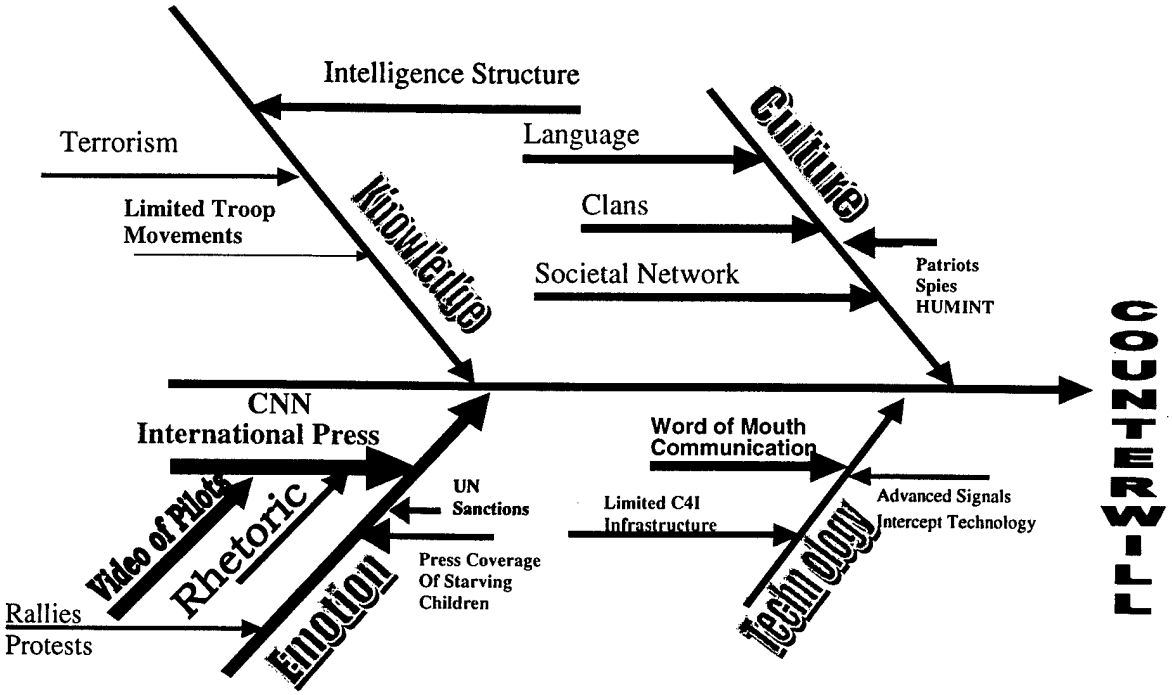


Figure 13. Somalia Event Fishbone.

Table 3. Somalia Event Matrix

Core Targets	Key Factors	Contributing Sub-factors	Counter-Influences	Counter Subfactors	Resulting Actions
Technology					
	Lacking typical C4I infrastructure		Standard US C4I communication structure		Non-standard or accepted communication practices, limited US monitoring capabilities
Emotion					
	Terrorist type of violence	Visual attacks on US pilots	Monitor situation	Limited action	Resulted in outrage of US citizens
	International Press	Aideed's pro-Somali rhetoric			Countered US rhetoric
	CNN	Videotapes of headless pilots being dragged through the streets	Modified Rules of Engagement	Viewed throughout the world	Limited US actions
Culture					
	Language	US forces are not normally trained in Somali dialects			Reduction of human-provided intelligence
	Decentralized societal networks		Superior information and dissemination techniques		No understanding of unit structure
	Clans				
Knowledge					
	Limited troop movements		Superior ISR technologies		Forces difficult to monitor for unusual activity

The run chart is a familiar evaluative tool which can be applied to some predictive analysis tasks. Very simple conceptually, run charts are plots of historical activity that highlight aberrant—or unusual—behaviors. In the example of the zealous analyst given earlier, a run chart showing accumulated data on activities in the area of interest, mapped over time, might have proven useful. Automatically generated from daily observations and available as a selectable screen display, planting and harvesting activity would have been displayed in their seasonal

context. The availability of such a decision-aiding tool would have added a dimension to the young analyst's diagnostic process which, in this case, was missing due to inexperience—a recurrent problem in the intelligence field as fewer experienced analysts are available compared to the number of novices (see Figure 14).

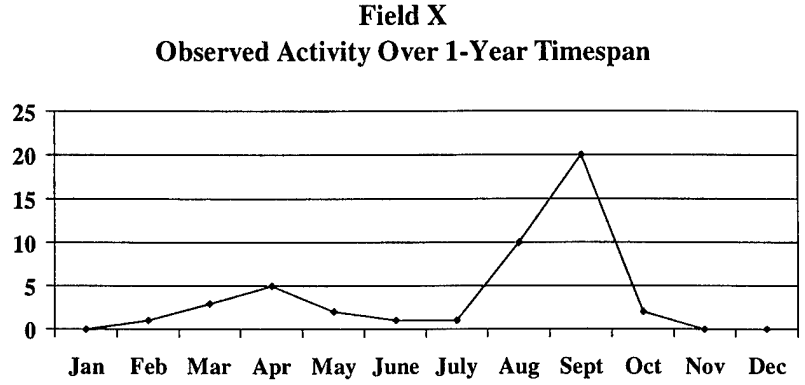


Figure 14. Notional Run Chart of Seasonally-Based Vehicle Activity.

IW modeling requires an understanding of man, machine, materials, and methods analogous to the understanding required for Deming's process improvement steps (as discussed in the section on cause and effect diagrams) and the modeling techniques of process or organizational improvement. These techniques clearly provide an effective methodology to identify the component influences or predictive elements for analytical and planning purposes. TECK influences, or predictive factors, can be extracted through decomposing and modeling intricate IW operations. Typically, some data is previously identified, but requires integration with other information to enhance its overall utility. Currently, operational commanders are able to obtain a partial understanding of the adversary through the Essential Elements of Information (EEI). EEIs are data identified as the "critical items of information regarding the enemy and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision" (*Joint Pub 1-02*, 1999). The EEI Responses are incorporated into the operational commander's knowledge base to clarify understanding of the operational picture as a whole and to help formalize operational planning and actions. Matrices effectively illustrate and organize relationships among multiple variables. IO applications can be mapped to specific OODA Loop modes and TECK influences (including the data contained in EEIs) in a deception matrix, as depicted in Figure 15.

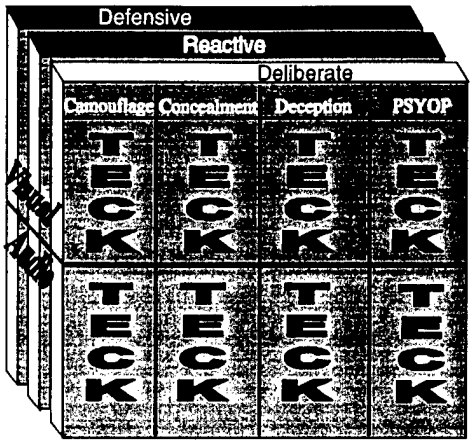


Figure 15. Deception Matrix.

A simple, generic matrix is supplied in Figure 15. For actual planning operations or for a specific reaction, a more detailed model would be required. These models, though rudimentary in nature, are the first stepping stone toward the creation of complex and automated models to help influence decision managers or to conduct perception management. For a more accurate or complete TECK model, complex meta-analysis tools are required. "Meta-analysis uses quantitative data, gathered from single studies, cumulates the data from across many studies, and estimates the true effects of treatments on dependent variables" (French & Bell, 1995).

The TECK Matrix in Figure 16 is designed to demonstrate how planning methods can aid the perception management process. This is an overly simplified version of the vastly complex planning criteria required for information operations. The matrix maps various types of deception techniques against the sensory inputs to be affected, the OODA Loop modes (deliberate, reactive, and defensive) to be influenced, and the key perception elements (technology, emotion, culture, and knowledge) to be manipulated.

The ratings in this chart are highly subjective, and are situation-dependent (i.e., tactical circumstances differ substantially from operational and strategic situations; offensive and defensive operations have different TECK objectives; therefore, each elicits a different set of reactions). The chart examines the potential use of various common techniques. Chaff is primarily a defensive reaction (shown in red in a color-coded matrix); it targets the "visual" sensors such as radar, and therefore, represents the technological aspect of the TECK model. Other techniques, such as PSYOP, may have little to no effect on defensive modes. Since PSYOP targets emotion and culture, although it has little effect on defensive modes, it can significantly

impact deliberate planning. Other techniques, such as concealment, may affect all DRDA modes and can defeat most technologies, but not without cost to the organization employing the technique. Continuous use of concealment limits one's ability to utilize what is being concealed.

Method/Techniques	Primary sensory mode affected	Deliberate	Reactive	Defensive	TECK
Active Cooling	Visual				T
Acoustic Generation	Auditory				TK
Camouflage	Visual				TK
Chaff	Visual				TK
Cipher/Encryption	Visual/Auditory				TK
Concealment	Visual				TK
Cyberwarfare	Visual/Auditory				TECK
Decoys	Visual				TK
Degaussing	Auditory				T
Dummies	Visual				TK
False Heat Source	Visual				T
Feints	Visual/Auditory				TECK
Fixed Target Indicators (FTIs)	Visual				T
Flares	Visual				T
Glint	Visual				TK
Hide	Visual				TECK
Imitative Electronic Deception (IED)	Auditory				TK
Jamming	Visual/Auditory				TK
Loudspeaker Broadcast	Auditory				ECK
Luminance Matching	Visual				TK
Manipulative Electronic Deception (MED)	Auditory				TK
Masking Emitters	Auditory				TKC
Misinformation	Visual/Auditory				ECKT
Moving Target Indicators (MTIs)	Visual				TK
Multispectral Close Combat Decoy (MCCD)	Visual				ETK
Multispectral Decoy	Visual				TK
Noise Suppression	Auditory				TK
Olfactory	Smell				CTEK
Optical Jammers	Visual				TK
Public Diplomacy (e.g., PSYOPS)	Visual/Auditory				ECK
Radio Broadcast	Auditory				ECK
Screens	Visual				TK
Shielding Defilade	Visual				TK
Signal Security	Auditory				TK
Simulative Electronic Deception	Auditory				TK
Smoke Screen	Visual				TK
Sonic	Auditory				TK
Spatial Manipulation	Visual				TK
Television Broadcast	Visual/Auditory				ECKT
Terrain Masking	Visual				TK

TECK = Technology, Emotion, Culture and Knowledge
TECK is listed in order of effectiveness (e.g., EC indicates Emotion and Culture are the prime targets)

DRDA Influence Key

Primary
Secondary
Minimal/No Effect

Figure 16. TECK Matrix.

Within process improvement, Business Process Reengineering applies engineering discipline to OD. DoD defines business process engineering in terms of functional process improvement. Functional process improvement is:

> "the application of a structured methodology to define a function's 'as is' and 'to be' environments, current and future mission needs and end user requirements; its objectives and strategy for achieving those objectives, and a program of incremental and evolutionary improvements to processes, data, and supporting Aids that are implemented through functional, technical, and economic analysis and decision-making" (OASD, 1995).

The Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence has developed process and data models to shape BPR efforts within the armed forces. Originally performed in the 1992-93 timeframe, the Business Process Reengineering Process Model is updated annually. The model provides a description of how to perform BPR, of the data relationships that support BPR, and includes an automated BPR toolset. It is intended for use in strategic planning, enterprise integration, and change management. The BPR Process Model uses a three-stage planning cycle, *Plan-Perform-Evaluate*, and divides planning into strategic and business planning. Strategic planning is outward-looking, context-based, and sets the vision for the future state. Business planning, analogous to tactical planning, is inward-looking and focuses resources on the steps required for vision attainment.

The BPR Process Model entails the use of requirements and organizational matrices, benchmarking, SWOT analysis (Strengths, Weakness, Opportunity, Threat), process flow models, and IDEF0—a functional decomposition tool. IDEF0 is an activity-based, iterative, structured analytical tool, developed by the Air Force, which captures inputs, constraints, outcomes, inter-relationships, and costs. Automated IDEF0, IDEF1 (the information modeler), and IDEF2 (the dynamics modeler), are all available in automated toolsets from a number of commercial sources. IDEF is the DoD standard modeling tool, and while it may be used for operational modeling, the rigorous nature of its structured analysis can influence the analyst to oversimplify complex activities. Originally developed for modeling manufacturing processes, it is somewhat linear in nature, and although it is a powerful tool, its inflexibility gives it limited utility modeling complex, dynamic processes in the presence of inevitable information deficits.

All services are authorized (and expected) to use the BPR Process Model; however, it is presently used for organization development rather than for operational planning. Its components have relevance for mission-oriented decision planning and the readily available, well-supported, structured analytical and planning process provides an opportunity for translation to the IW domain. In particular, the SWOT analysis is a tool which bears promise as an element within predictive analysis.

Another potentially useful tool for predictive analysis is the engineering model, the decision-maker's logic tree, or decision chart. Starting from a decision point, all possible courses of action are listed, and each course of action shows its own set of choices, providing multiple possible paths. If data exist to support it, probability of selection (based on the historical data) is assigned to each step (node) on the path. The sum of probabilities always equals 100%. Multiple choices mean each choice has a smaller probability of being selected, and therefore, that each outcome has a smaller probability of occurrence. If based on historical data, the sum of the outcomes (calculated by multiplying the values along a decision path) shows the percentage of times a given outcome occurred and can be used to evaluate the likelihood of its reoccurrence. While the fallacy of using historical data for probability calculation is that there is no real way, within the decision chart, of showing influential factors, the decision chart may be drawn based upon a separate analysis of previously determined influences, or it may be used merely to enumerate and track possible choices and outcomes (see Figure 17).

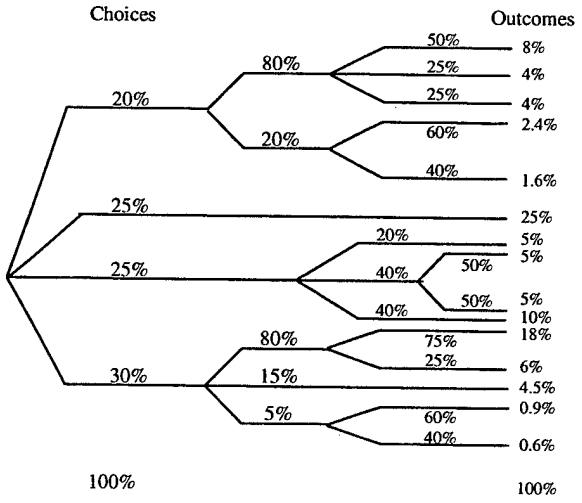


Figure 17. Decision Tree Showing Decision Branches With Associated Probabilities.

In 1995, the Air Force began a one-year study of the concepts, capabilities, and technologies the U.S. would require for air and space dominance 30 years in the future. Titled *AF 2025*, the study was conducted jointly by Air University's Air War and Air Command and Staff Colleges, the Air Force Institute of Technology, the Air Force Academy, and Air Force Reserve Officer Training Corps cadets at colleges and universities across the nation. The project was distilled to an executive summary and 41 papers, all of which are available at the *AF 2025* site on the World Wide Web. Included in the collection are papers on both *value-focused thinking* and on *wisdom warfare.*

In value-focused thinking, the analyst identifies the decision-maker's values and organizes them as a hierarchy of objectives. The objectives at the top of the hierarchy represent values that are most important to the decision-maker, and which can be considered strong motivating forces. "Objectives are decomposed until force qualities can be specified and measured. Weights are assigned to signify the relative importance of objectives at every level" (Jackson, Jones & Lehmkuhl, 1996). Evaluations are scored based on computations of the relative weights. With a clear statement of objective to serve as the overarching principle, value-focused thinking can support analysis from bottom-up rather than the more usual top-down. Used for evaluating competing strategies, it can also be adapted for use in predictive analysis. The cultural values of the adversary, when modeled and weighted through the value-focused thinking structure, can become predictors of likely behaviors and can be used both to anticipate adversarial activity and to plan effective tactics for behavior modification. A value-focused analysis of the character of the Kosovar Serbs and the Serbian leader, Slobodan Milosevic, might have yielded useful insights during the recent NATO intervention. Particular notice might have been taken, for example, of the cultural difference which makes victimization a unifying force among the Serbs, in contrast to the widely (but not universally) held U.S. preference to deny victimization in order to maintain the appearance of autonomy. Similar cultural insights might become useful tools in the hands of the IO tactician.

Wisdom warfare architecture combines *knowledge* (data collection/organization systems that turn raw data into usable information), *wisdom* (modeling and simulation tools and other aids that facilitate human interaction with knowledge to make the best decisions), and *the human system integration* (all systems necessary to shape information as needed to support sound human decision-making). The information explosion has created an overwhelming rain of data on the

decision-maker. Sensors collect observable phenomena and produce event data. Analyses are performed by humans who, aided by data fusion systems, correlate and associate relevant information to enhance situational understanding. Automated decision aids and forecasting tools provide wisdom support, which, coupled with human judgement mediated by experience, creativity, and intuition, make better decisions obtainable more quickly. Wisdom warfare architecture improves warfighters' judgement by synthesizing information and modeling and simulating scenarios to provide advice, options, and probabilities of occurrence. Applied to predictive analysis in information operation planning, for example, a wisdom system containing archived past forecasts and outcomes can assist the commander or planner to forecast and categorize possible enemy courses of action as well as to explore multiple, alternative friendly courses of action (see Figure 18; Murphy, Bender, Shaefer, Shepard & Williamson, 1996).

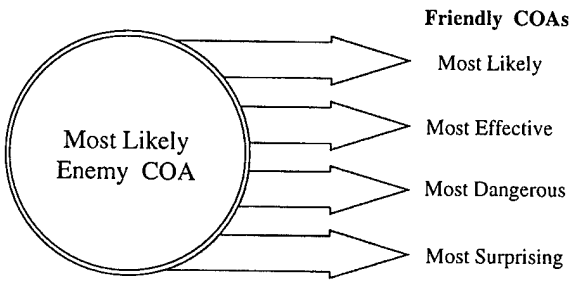


Figure 18. Course of Action Development (Murphy et al., 1996).

One commercial-off-the-shelf software product bears particular promise for operational decision-making modeling applications. Imagine That, Inc. markets a series of automated modeling and simulation tools based on the software package, *Extend*, a dynamic, iconic simulation environment with a built-in development system which permits the simulation of discrete event processes, continuous processes, and combined discrete event/continuous processes and systems. It is used for engineering design, scientific experimentation, environmental studies, operations research, and performance evaluation to validate theories, diagnose potential problems, and find best performance/cost ratios. Designed for reengineering business processes, *Extend+BPR* can be used for planning and decision support, operations and production systems, cycle time reduction, continuous improvement, human performance modeling, activity-based costing, and productivity and quality improvements. Its multiple libraries of "drag and drop" pre-built event blocks, iconic and "functional blueprint" pictorial capabilities provide both flexibility and ease of use. Its potential utility for information operations includes both predictive analysis

of adversary behaviors and predictive analysis of mission-planning, as it allows the planner to build realistic models showing relationships, dependencies, vulnerabilities, and constraints. The modeling process is shaped by the modeler rather than the software, so the tool does not artificially limit, inhibit, or distort the model.

The short review of models and modeling tools in the preceding pages reveal a number of possibilities for creative applications in information operations. The key to making the models work is to integrate a thorough understanding of the human decision-making process with the decision-making modeling tools. Figure 19 depicts the complexities of the interaction between technology and the human decision-maker within the information battlespace.

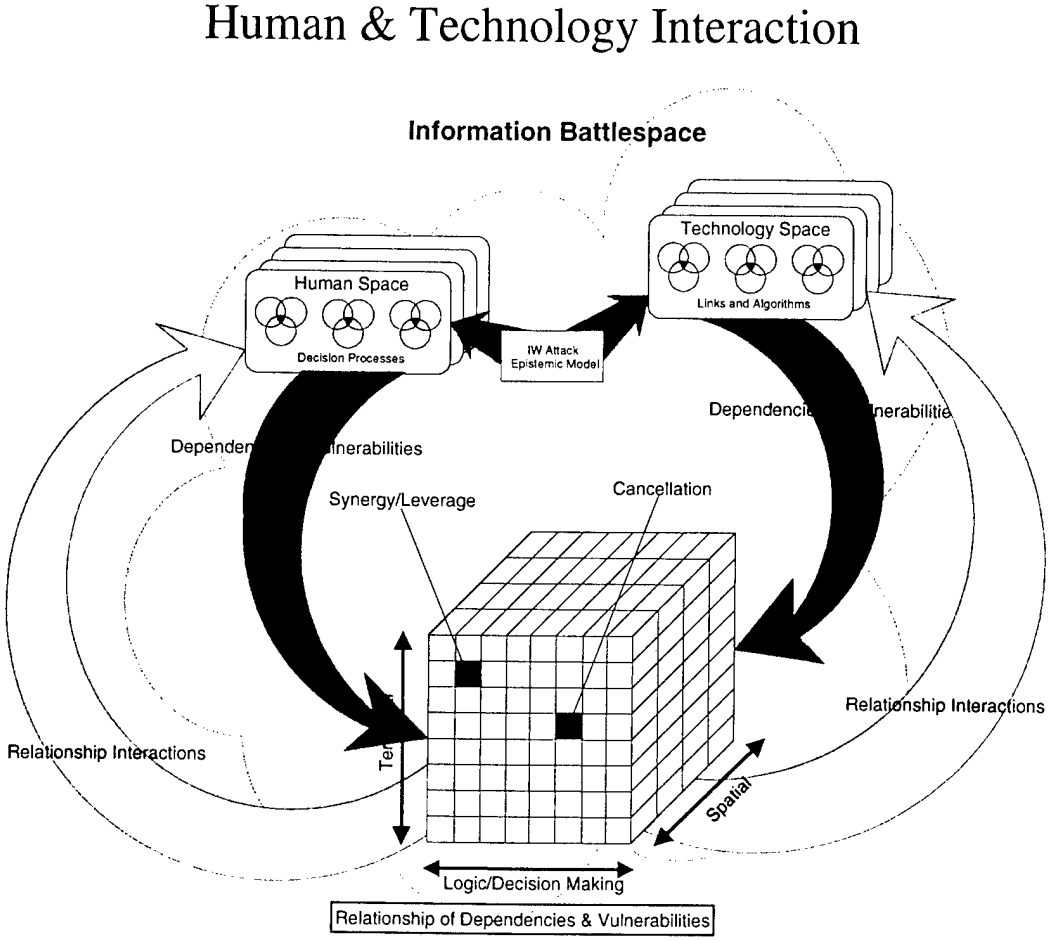


Figure 19. Human and Technology Interaction—Decision-Making Matrix for the Information Battlespace.

A simpler matrix (Figure 20) illustrates the interface of the TECK core elements, the BPR and other models. As the complex inter-relationships shown in Figure 19 suggest, any attempt to

create predictive analytical tools will require the use of multiple models in order to capture the nuances of the decision-making process with sufficient verisimilitude to ensure any degree of accuracy. The challenges and opportunities offered by the interface of the perceptual process mediators (represented by *technology, emotion, culture,* and *knowledge*) with the decision process require serious consideration. Classification of deliberative, reactive, and defensive actions permits future studies to focus not just upon one phase of the OODA Loop activity cycle, but allows the researcher to further narrow the field of view to a recognizable category of action. Discrete action types may be studied concurrently with isolated TECK influences, offering a more manageable methodology for scientific analysis of the decision-making process.

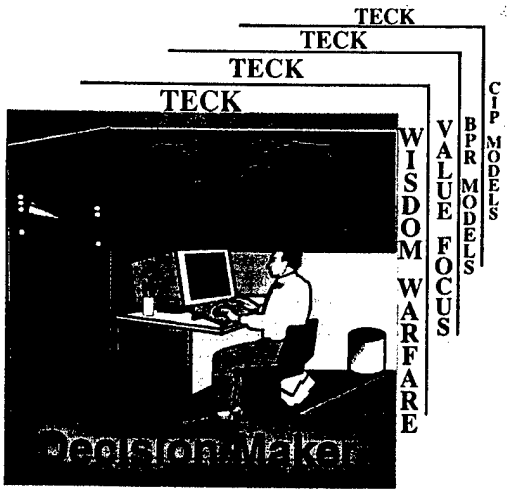


Figure 20. Decision-Making Matrix for Process Modeling Tools.

The decision-making process itself is not well understood at this time. The past and present studies sponsored by the Air Force Research Laboratory have underlined the need for further study of both naturalistic decision-making—and the factors that shape decisions—and adversarial decision-making—a problem set which includes the requirement to fully understand (and exploit) the effects of cultural differences. The selective use of modeling techniques will support the requisite basal human factors research, as well as the development of well designed advanced aiding technologies, whether facilitative (decision-making aids) or predictive (adversarial behavior analysis and forecast). Any serious attempt to build an effective predictive model of adversarial behavior of *any* degree of authenticity must be based on Sun Tzu's well known observation that in order to achieve victory in conflict, one must know one's enemy *and* one must know one's self.

CONCLUSION

Information warfare is designed to attack the decision-making process. Information operations—the methodology of IW—is evolving at a rapid pace, as much driven by the specter of documented adversarial activities against which we must protect ourselves as led by the vision of opportunities we must grasp in order to maintain the relative security of our current military capability. Offensive and defensive information operations can successfully attack and alter the adversary's decision-making process—the key to both the adversary's ability and willingness to engage in hostilities. Coercing adversaries to modify or limit their hostile activities becomes a positive force multiplier that saves both lives and resources. Thus, in order to maximize the efficacy of IO, a keen understanding of the decision-making process is required.

The decision-making process, as modeled by the OODA Loop, is composed of the *Observe, Orient, Decide,* and *Act* decision activities. Moderating the decision-making process are those elements that make us individuals, including our access to and skill with modern technology and equipment, the strengths and vulnerabilities of our emotions, our cultural experience, and our knowledge base (the TECK core elements). The decision-making process is not a single iterative OODA Loop process but a multidimensional, linked, iterative process containing multiple overlapping deliberate, reactive, and defensive OODA Loops. A focus of research by all of the Air Force's schools of advanced military studies as well as its laboratory facilities, determining the way to "optimize" one's own OODA Loop—while simultaneously "degrading" the OODA Loop of one's adversary—is the very heart of military strategy past, present, and future. It is the ultimate goal of all IO planning and a topic of current discussion in the published papers of the Air Force's massive operations research and forecast effort, *AF 2025.*

The application of IO tools based on predictive OODA Loop models will eventually provide a high return in information operations. We are no longer facing simplistic IO techniques, and we can no longer afford to apply our own IO without full knowledge both of our own and our adversary's decision-making processes. IO applications are only effective if there is a complete understanding of the adversary. Highly evolved technological solutions may not always be the answer, as we discovered from our operations in Somalia and Kosovo. Understanding the adversary's decision-making process and predicting how they will react is the

key to development of effective IO. While operational commanders are able to obtain a partial understanding of the adversary through the EEI process, in order to exploit the adversary's decision process more efficiently and effectively, operational commanders need better information. This includes a full understanding of the adversary's TECK core and the use of appropriate predictive models and intervention tools.

There is, as yet, a lack of effective tools to model intricate IW operations. In reality, modeling aspects of information operations is analogous to modeling business or organizational improvement. Information warfare planning, like process reengineering, requires an understanding of man, machine, materials, and methods. Investigating the use of appropriate modeling and intervention techniques will yield a more effective set of tools to structure and sharpen both strategic and tactical IW operational planning.

This exploratory work has identified the need for more intricate models to aid in both strategic and tactical planning and adversarial decision-making. Equally, it has noted the need for models that will help us develop a better understanding of the minds of our potential adversaries. The modeling concepts provided here are neither an exhaustive list, nor are their uses discussed in detail; they certainly do not constitute a complete solution to IW or IO planning problems. However, the examination of these models does demonstrate the need for further study. It is clear that modeling for predictive analysis is critical to effective IW, but effective modeling will not be accomplished without laying the proper groundwork. Prior to establishing models and applying tools, in-depth human factors analysis of the human decision-maker is required—both to increase our understanding of our own and our potential adversary's decision-making capabilities, strengths, and weaknesses and to identify the most effective predictive analysis tools to support information operations. Relying on new advanced sensor technologies is not the sole answer. Information about adversarial activity is only useful if effective countermeasures can be identified—predictive analysis is critical to successful information operations. Predictive analysis modeling will provide the leverage to make IW the force multiplier it is touted to be.

REFERENCES

Air Land Sea Application Center. (no date). *Executive Summary, Multiservice Tactics, Techniques and Procedures for CCD Employment in C2W).* Washington, DC: author. Available online at: http://www.dtic.mil/alsa/ccd.htm

Alberts, D. S. (April 1996). *The unintended consequences of information age technologies* [online book]. Ft. Leslie J. McNair, Washington, DC: National Defense University Press. Available online at: http://www.ndu.edu/inss/books/uc/uchome.html

Boyd, J. (1987). *A Discourse on Winning and Losing.* [Unpublished briefing.] Air University Library Report No. MU 43947. Maxwell AFB, AL: Air University.

Brennan, R. R. & Ellis, E. (April 18, 1996). *Information warfare in multilateral peace operations: A case study of Somalia.* Available online at: http://sac.saic.com/SOMALIA.HTM

Bunker, R. J. (Autumn, 1996). Advanced battlespace and cybermaneuver concepts: Implications for Force XXI. *Parameters*, pp. 108-119.

Bureau of Reclamation. (no date). *Decision Process Guidebook* [on-line document]. Washington, DC: U.S. Department of the Interior. Available online at: http://www.usbr.gov/guide/toolbox/toollist.htm

Clemson University. (1997). *Deming Electronic Network Website.* Clemson, SC: Clemson University, Industrial Engineering Dept. Available online at: http://deming.eng.clemson.edu/pub/den/index.html

Covey, Steven (1990). *The 7 habits of highly effective people.* New York: Fireside.

Damasio, A. R. (1994). *Descartes' error: Emotion, reason, and the human brain* (pp. xii). New York: Avon Books.

Doherty, J. (Coord.). (Fall 1994). *TQM (Total Quality Management) Toolkit, Version 1.* Cambridge, MA: Massachusetts Institute of Technology Information Systems. Available online at: http://web.mit.edu/is/help/tqm/

Dulles, A. W. (1968). *Great true spy stories.* New York: Ballantine Books.

Fine, E. (August 1997). Fine-tuned SPC: Solve problems with the appropriate SPC tool. *Quality Magazine.* Available online at: http://www.qualitymag.com/0897ft.html

Fisher, D. (1983). *The war magician.* New York: Coward-McCann, Inc.

French, W. L. & Bell, C. H. (1995). *Organization development: Behavioral science interventions for organization improvement.* Englewood Cliffs, NJ: Prentice Hall.

Goldstein, F. L. & Findley, B. F. (Eds.). (September 1996). *Psychological operations: Principle and case studies*. Maxwell AFB, AL: Air University Press.

Hoffman, P. (no date). *The process improvement guide*. Wright-Patterson AFB, OH: TQM Office.

Holcombe, M. & Stein, J. (1996) *Presentations for decision makers* (3rd ed.). New York: Van Nostrand Reinhold.

Holmes, S. (1994). *The quality approach* (2nd ed.). Maxwell AFB, AL: Air Force Quality Institute.

Imagine That, Inc. (no date). *About Extend*. [Product description]. Available online at: http://www.imaginethatinc.com/extend_details.html

Jackson, J., Jones, B. & Lehmkuhl, L. (1996). *An operational analysis for Air Force 2025: An application of value-focused thinking to future air and space capabilities*. Maxwell AFB, AL: Air University. Available online at: http://www.au.af.mil/au/2025/volume4/chap03/v4c3-01.htm

Jervis, R., Lebow, R., & Stein, J. (1985). *Psychology and deterrence*. Baltimore, MD: Johns Hopkins University Press.

Joint Chiefs of Staff. (1996). *Joint Vision 2010*. Washington, DC: Author. Available online at: http://www.dtic.mil/doctrine/jv2010/jvpub.htm

Joint Chiefs of Staff. (1998) *Joint Publication 3-13, Joint Doctrine for Information Operations*. Washington, DC: GPO. Available online at http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf

Joint Chiefs of Staff. (as emended, 1999). *Joint Publication 1-02, DOD Dictionary of Military and Associated Terms*. Washington, DC: GPO. Available online at: http://www.dtic.mil/doctrine/jel/doddict/

Klein, G. (1997). *Implications of the naturalistic decision making framework for information dominance*. Report No. AL/CF-TR-97-0155. Wright Patterson AFB, OH: Armstrong Laboratory.

Llinas, J., Drury, C., Bialas, W. & Chen, A. (1998). *Studies and analyses of vulnerabilities in aided adversarial decision-making*. Wright-Patterson AFB, OH: Air Force Research Laboratory, Human Effectiveness Directorate.

Murphy, E., Bender, G., Shaefer, L., Shepard, M., & Williamson, C. (1996). *Information operations: Wisdom warfare for 2025*. Maxwell AFB, AL: Air University. Available online at: http://www.au.af.mil/au/2025/volume1/chap01/v1c1-01.htm

Office of the Deputy Assistant Secretary of Defense (OASD). (1995). *Business Process Reengineering (BPR) Process Model, Formal Update, Version 3*. Washington, DC: OASD/Information Management. Available online at: http://www.dtic.mil/c3i/bprcd/5085.htm

Sick, G. (1985). *All fall down: America's tragic encounter with Iran.* New York: Random House. Excerpted online at: http://infoplease.lycos.com/ce5/CE025947.html

Spinney, F. C. (1997). *Evolutionary epistemology: A personal interpretation of John Boyd's Destruction and Creation.* [Briefing]. Available online at: http://www.belisarius.com/modern_business_strategy/ev_epis/evolutionary_1.htm

Strategic Communications. (1998). *Presentation Planning—Draw A Logic Tree.* [Online article]. Available online at: http://www.strategiccomm.com/logictree.html

Sun Tzu. (1963). *The art of war.* (S. B. Griffith, Trans.). Oxford: Oxford University Press. (Sources differ, but modern estimates place publication of the original in the 4th century BCE.)

U.S. Air Force. (1997). *Air Force Doctrine Document (AFDD) 1. Air Force Basic Doctrine.* Maxwell AFB, AL: Headquarters Air Force Doctrine Center.

U.S. Air Force. (1992). *Air Force Manual (AFM) 1-1, Volume I: Basic Aerospace Doctrine of the United States Air Force.* Washington, DC: Department of the Air Force.

U.S. Air Force. (1992). *Air Force Manual (AFM) 1-1, Volume II: Basic Aerospace Doctrine of the United States Air Force.* Washington, DC: Department of the Air Force.

U.S. Air Force. (1994). *Air Force Instruction (AFI) 32-4007: Camouflage, Concealment and Deception.* Washington, DC: Department of the Air Force.

U.S. Air Force. (1997). *Air Force Instruction (AFI) 10-704: Military Deception Program.* Washington, DC: Department of the Air Force.

U.S. Army. (date unknown). *Field Manual (FM) 90-2: Battlefield Deception.* Washington, DC: Department of the Army.

Virgil. (1965). *The Aeneid.* (J. Dryden, Trans.; with notes by R. Fitzgerald, Ed.). New York: Macmillan. (Original work published in 19 BCE.)

von Clausewitz, C. (1984). *On war.* (M. Howard & P. Paret, Trans./Eds.). Princeton, NJ: Princeton University Press. (Original work published in 1832.)

Whitaker, R. D. & Kuperman, G. G. (October 1996). *Cognitive engineering for information dominance: A human factors perspective.* Report No. AL/CF-TR-96-0155. Wright-Patterson AFB, OH: Armstrong Laboratory.

Widnall, S. & Fogleman, R. R. (1996). *Cornerstones of information warfare.* Available online at: http://www.af.mil/lib/corner.html

ACRONYM LIST

AFI	Air Force Instruction
AFM	Air Force Manual
BPR-	Business Process Reengineering
C2W	Command and Control Warfare
C4I	Command, Control, Communications, Computers, and Intelligence
CCD	Camouflage, Concealment, and Deception
CCDD	Camouflage, Concealment, Denial, and Deception
MCCD	Multispectral Close Combat Decoy
COA	Course of Action
DM	Decision-Making
DOD	Department of Defense
DRDA	Deliberate, Reactive, and Defensive Acts
EEI	Essential Elements of Information
FM	Field Manual (U.S. Army)
FTI	Fixed Target Indicator
HUMINT	Human Intelligence
IA	Imagery Analyst
IED	Imitative Electronic Deception
IO	Information Operations
IP	Information Protect
IPB	Intelligence Preparation of the Battlefield
IR	Infrared
ISR	Intelligence, Surveillance, and Reconnaissance
IW	Information Warfare
JFC	Joint Forces Commander[s]
MED	Manipulative Electronic Deception
MTI	Moving Target Indicator
NDM	Naturalistic Decision-Making
OASD	Office of the Assistant Deputy Secretary of Defense
OD	Organization Development

OODA	Observe, Orient, Decide, Act
PSYOP	Psychological Operations
ROE	Rule[s] of Engagement
SIGINT	Signals Intelligence
SOP	Standard Operating Procedure
SWOT	Strengths, Weakness, Opportunity, Threat
TECK	Technology, Emotion, Culture, Knowledge
TQM	Total Quality Management

GLOSSARY[1]

Active Cooling: A deception technique that conceals or breaks up thermal signatures by cooling heat sources to fool infrared sensors.

Acoustic Generation: The production of sound waves to spoof or confuse technology (such as torpedo decoys.

Battlespace: The environment in which humans, and their machines operate.

Camouflage: (DOD, NATO) The use of natural or artificial material on personnel, objects, or tactical positions with the aim of confusing, misleading, or evading the enemy. See also countersurveillance. (*Joint Pub. 1-02*). It enables the most vulnerable of creatures to remain undetected by its predators.

Chaff: (DOD) Radar confusion reflectors, which consist of thin, narrow metallic strips of various lengths and frequency responses, used to reflect echoes for confusion purposes. (*Joint Pub. 1-02*)

Cipher: (DOD) Any cryptographic system in which arbitrary symbols or groups of symbols, represent units of plain text of regular length, usually single letters, or in which units of plain text are rearranged, or both, in accordance with certain predetermined rules. (*Joint Pub. 1-02*)

Course of Action: (DOD) 1. A plan that would accomplish, or is related to, the accomplishment of a mission. 2. The scheme adopted to accomplish a task or mission. It is a product of the Joint Operation Planning and Execution System concept development phase. The supported commander will include a recommended course of action in the commander's estimate. The recommended course of action will include the concept of operations, evaluation of supportability estimates of supporting organizations, and an integrated time-phased data base of combat, combat support, and combat service support forces and sustainment. Refinement of this data base will be contingent on the time available for course of action development. When approved, the course of action becomes the basis for the development of an operation plan or operation order. Also called COA. (*Joint Pub. 1-02*)

---

[1] Where so cited, definitions are taken in whole or in part from the Joint Chiefs of Staff's *Joint Publication 1-02, DOD Dictionary of Military and Associated Terms* (1999). Other definitions are similarly cited, or are provided by the authors.

Communications Security: (DOD) The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes: crypto-security, transmission security, emission security, and physical security of communications security materials and information. a. crypto-security--The component of communications security that results from the provision of technically sound crypto-systems and their proper use. b. transmission security--The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than crypto-analysis. c. emission security--The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems. d. physical security--The component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (*Joint Pub. 1-02*)

Concealment: (DOD, NATO) The protection from observation or surveillance. See also camouflage; cover; screen. (Hides critical components and denies access to potential targets from observation or surveillance.) (*Joint Pub. 1-02*)

Counter-Deception: (DOD) Efforts to negate, neutralize, diminish the effects of, or gain advantage from, a foreign deception operation. Counter-deception does not include the intelligence function of identifying foreign deception operations. See also deception. (*Joint Pub. 1-02*)

Deception: (DOD, NATO) Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. See also counter-deception; military deception. (*Joint Pub. 1-02*)

Deception Action: (DOD) A collection of related deception events that form a major component of a deception operation. (*Joint Pub. 1-02*)

Deception Concept: (DOD) The deception course of action forwarded to the Chairman of the Joint Chiefs of Staff for review as part of the CINC's Strategic Concept. (*Joint Pub. 1-02*)

Deception Event: (DOD) A deception means executed at a specific time and location in support of a deception operation. (*Joint Pub. 1-02*)

Deception Means: (DOD) Methods, resources, and techniques that can be used to convey information to the deception target. There are three categories of deception means: a. physical means--Activities and resources used to convey or deny selected information to a foreign power. (Examples: military operations, including exercises, reconnaissance, training activities, and movement of forces; the use of dummy equipment and devices; tactics; bases, logistic actions, stockpiles, and repair activity; and test and evaluation activities.) b. technical means--Military material resources and their associated operating techniques used to convey or deny selected information to a foreign power through the deliberate radiation, reradiation, alteration, absorption, or reflection of energy; the emission or suppression of chemical or biological odors; and the emission or suppression of nuclear particles. c. administrative means--Resources, methods, and techniques to convey or deny oral, pictorial, documentary, or other physical evidence to a foreign power. (*Joint Pub. 1-02*)

Deception Objective: (DOD) The desired result of a deception operation expressed in terms of what the adversary is to do or not to do at the critical time and/or location. (*Joint Pub. 1-02*)

Deception Story: (DOD) A scenario that outlines the friendly actions that will be portrayed to cause the deception target to adopt the desired perception. (*Joint Pub. 1-02*)

Deception Target: (DOD) The adversary decision-maker with the authority to make the decision that will achieve the deception objective. (*Joint Pub. 1-02*)

Decoy: (DOD, NATO) An imitation in any sense of a person, object, or phenomenon which is intended to deceive enemy surveillance devices or mislead enemy evaluation. (*Joint Pub. 1-02*)

Desired Perception: (DOD) In military deception, what the deception target must believe for it to make the decision that will achieve the deception objective. (*Joint Pub. 1-02*)

Decision-Making Process: The procedures involved to conduct an independent thought process or action and plan from inception to completion.

Degaussing: (DOD) The process whereby a ship's magnetic field is reduced by the use of electromagnetic coils, permanent magnets, or other means. (*Joint Pub. 1-02*)

Electromagnetic Deception: (DOD) The deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an enemy or to enemy electromagnetic-dependent weapons, thereby degrading or neutralizing the enemy's combat capability. Among the types of electromagnetic deception are: a. manipulative electromagnetic deception--Actions to eliminate revealing, or convey misleading, electromagnetic telltale indicators that may be used by hostile forces. b. simulative electromagnetic deception--Actions to simulate friendly, notional, or actual capabilities to mislead hostile forces. c. imitative electromagnetic deception--The introduction of electromagnetic energy into enemy systems that imitates enemy emissions. See also electronic warfare. (*Joint Pub. 1-02*)

Electronic Warfare: (DOD) Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. a. electronic attack. That division of electronic warfare involving the use of electromagnetic, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. Also called EA. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams). b. electronic protection. That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. Also called EP. c. electronic warfare support. That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support provides information required for immediate decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called ES. Electronic warfare support data can be used to produce signals intelligence, both communications intelligence, and electronics intelligence. See also command and control warfare; communications intelligence; directed

energy; directed-energy device; directed-energy warfare; directed-energy weapon; electromagnetic compatibility; electromagnetic deception; electromagnetic hardening; electromagnetic jamming; electromagnetic spectrum; electronics intelligence; frequency deconfliction; signals intelligence; spectrum management; suppression of enemy air defenses. (*Joint Pub. 1-02*)

Encrypt: (DOD) To convert plain text into unintelligible forms by means of a cryptosystem. (Note: The term "encrypt" covers the meanings of "encipher" and "encode.") (*Joint Pub. 1-02*)

Essential Elements of Information: (DOD) The critical items of information regarding the enemy and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision. Also called EEI. (*Joint Pub. 1-02*)

False Heat Source: An infrared generator used to deceive infrared sensors.

Feint: (DOD) In military deception, an offensive action involving contact with the adversary conducted for the purpose of deceiving the adversary as to the location and/or time of the actual main offensive action. (*Joint Pub. 1-02*)

Fixed Target Indicator: Fixed target indicators are devices that provide the radar signature for stationary targets. Also called FTI. (*Joint Pub. 1-02*)

Flares: A pyrotechnics device used for a variety of defense applications including an expendable defensive measure to decoy IR sensors.

Glint: Random motion of the apparent center of reflection from a target resulting from scintillation.

Human Intelligence: (DOD, NATO) A category of intelligence derived from information collected and provided by human sources. Also called HUMINT. (*Joint Pub. 1-02*)

Imitative Electronic Deception (IED): (DOD) The deliberate radiation, reradiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an enemy or to enemy electromagnetic-dependent weapons, thereby degrading or neutralizing the enemy's combat capability. Among the types of electromagnetic deception are: a. manipulative electromagnetic deception--Actions to eliminate revealing, or convey misleading, electromagnetic telltale indicators that may be used by hostile

forces. b. simulative electromagnetic deception--Actions to simulate friendly, notional, or actual capabilities to mislead hostile forces. c. imitative electromagnetic deception--The introduction of electromagnetic energy into enemy systems that imitates enemy emissions. (*Joint Pub. 1-02*)

Information Operations: Those methods, actions or techniques utilized to conduct either offensive or defensive information warfare.

Information Superiority: (DOD) The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (*Joint Pub. 3-13*)

Information Warfare: (DOD) Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks. (*Joint Pub. 1-02*)

Intelligence Preparation of the Battlefield (IPB): (DOD) Analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive database for each potential area in which a unit may be required to operate. The database is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and presents it in graphic form. Intelligence preparation of the battlespace is a continuing process. (*Joint Pub. 1-02*)

Loudspeaker Broadcast: A technique used to transmit verbal messages or noises. Commonly used in psychological operations.

Luminance Matching: A deception technique that incorporates contrast and spatial manipulation to make an object blend into the background.

Manipulative Electronic Deception: A form of electronic deception used to manipulate, falsify, and distort the electromagnetic profile of friendly forces. Uses techniques such as false traffic signals, false peaks in communications, traffic padding, routing, electronic cover, controlled breaches of security and an increase or decrease in activity of noncommunications emitters. Also called MED.

Masking Emitter: A deception technique used to hide true electronic signatures by emitting false signatures.

Misinformation: The product of a ruse. Purposely feeding the enemy incorrect information to gain an advantage.

Military Deception: (DOD) Actions executed to deliberately mislead adversary military decision-makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or in-actions) that will contribute to the accomplishment of the friendly mission. The five categories of military deception are: a. strategic military deception--Military deception planned and executed by and in support of senior military commanders to result in adversary military policies and actions that support the originator's strategic military objectives, policies, and operations. b. operational military deception--Military deception planned and executed by and in support of operational-level commanders to result in adversary actions that are favorable to the originator's objectives and operations. Operational military deception is planned and conducted in a theater of war to support campaigns and major operations. c. Tactical military deception--Military deception planned and executed by and in support of tactical commanders to result in adversary actions that are favorable to the originator's objectives and operations. Tactical military deception is planned and conducted to support battles and engagements. d. Service military deception--Military deception planned and executed by the Services that pertain to Service support to joint operations. Service military deception is designed to protect and enhance the combat capabilities of Service forces and systems. e. military deception in support of operations security (OPSEC)--Military deception planned and executed by and in support of all levels of command to support the prevention of the inadvertent compromise of sensitive or classified activities, capabilities, or intentions. Deceptive OPSEC measures are designed to distract foreign intelligence away from, or provide cover for, military operations and activities. See also deception. (*Joint Pub. 1-02*)

Moving Target Indicator: (DOD, NATO) A radar presentation which shows only targets which are in motion. Signals from stationary targets are subtracted out of the return signal by the output of a suitable memory circuit. Also called MTI. (*Joint Pub. 1-02*)

Multispectral Close Combat Decoy: Simulates both physical and infrared signatures of selected modified tables of equipment. Also called MCCD.

Multispectral Decoy: Simulates both physical and infrared signatures of selected modified tables of equipment. Also called MSD.

Noise Suppression: A technique used to prevent sounds that will give away the true operation. Methods include noise discipline and padding.

Olfactory: A deception technique used to project odor that is consistent with the visual, sonic and electronic methods used.

OODA Loop: *Observe, Orient, Decide, Act* template for modeling the decision-making process, created by Col John Boyd to describe the decision-making processes of combat pilots.

Optical Jammers: Defensive countermeasures used to protect against surface to air (SAM) missiles.

Operational Level of War: Military leaders must use their forces to achieve objectives that support the political and strategic goals for which their nation is fighting. Commanders attempt to decide when, where, and under what conditions their forces will attack or defend to support those goals. In the conduct of operations, the enemy presents enormous imponderables, because he is a living, breathing opponent who aims to thwart our every move by maneuvering and acting in accordance with his own designs and purposes, not all of which we may expect. The building blocks utilized in operational plans and execution are the tactics of the forces and the weapon systems of the different services.

Psychological Operations: (DOD) Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called PSYOP. (*Joint Pub. 1-02*)

Radio Deception: (DOD) The employment of radio to deceive the enemy. Radio deception includes sending false dispatches, using deceptive headings, employing enemy call signs, etc. See also electronic warfare. (*Joint Pub. 1-02*)

Rules of Engagement: (DOD) Directives issued by competent military authority which delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered. Also called ROE. See also law of war. (*Joint Pub. 1-02*)

Screen: (DOD, NATO) 1. An arrangement of ships, aircraft and/or submarines to protect a main body or convoy. 2. In cartography, a sheet of transparent film, glass or plastic carrying a "ruling" or other regularly repeated pattern which may be used in conjunction with a mask, either photographically or photomechanically, to produce areas of the pattern. See also halftone screen. 3. In surveillance, camouflage and concealment, any natural or artificial material, opaque to surveillance sensor(s), interposed between the sensor(s) and the object to be camouflaged or concealed. See also concealment. 4. A security element whose primary task is to observe, identify and report information, and which only fights in self-protection. (*Joint Pub. 1-02*)

Signals Intelligence: (DOD) 1. A category of intelligence comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. 2. Intelligence derived from communications, electronics, and foreign instrumentation signals. Also called SIGINT. See also communications intelligence; electronics intelligence; intelligence; foreign instrumentation signals intelligence. (*Joint Pub. 1-02*)

Shielding Defilade: A barrier used to shield an object from being detected.

Simulative Electromagnetic Deception: A form of electronic deception used to mislead the enemy as to actual composition, deployment and capabilities of friendly forces. Simulates nonexisting units or capabilities at false location, and simulates communications and noncommunications emitters. Also called SED.

Smoke Screen: (DOD, NATO) Cloud of smoke used to mask either friendly or enemy installations or maneuvers.

Sonic: A deception technique utilizing sound projection to produce battlefield noises. It is directed against the enemy's sound ranging gear and the human ear.

Spatial Manipulation: A deception technique used to break the pattern of an object or to blend it with its surroundings.

Spot Jamming: (DOD, NATO) The jamming of a specific channel or frequency. (*Joint Pub. 1-02*)

Standard Operating Procedure: (DOD, NATO) A set of instructions covering those features of operations which lend themselves to a definite or standardized procedure without loss of

effectiveness. The procedure is applicable unless ordered otherwise. Also called SOP (*Joint Pub. 1-02*)

Strategic Level of War: Military and civilian leaders determine crucial priorities between theaters and service efforts, set the focus of military operations, and define the military goals necessary to achieve political objectives. On this level, commanders decide how best to use available resources to achieve larger objectives.

Tactical Level of War: (AFM1-1) Deals with the basic, fundamental employment of weapons and troops to defeat, kill, and destroy the enemy. Skillful tactical employment is crucial to the conduct of operations. It is on the operational and tactical levels that battlefield success rests. But commanders must recognize that battlefield success is meaningful only within the larger context of sound strategic and political objectives. (*Air Force Manual 1-1*)

Tactical Deception Group: (DOD) A task organization that conducts deception operations against the enemy, including electronic, communication, visual, and other methods designed to misinform and confuse the enemy. A deception scheme developed during the estimate process in sufficient detail to permit decision-making. At a minimum, a deception course of action will identify the deception objective, the deception target, the desired perception, the deception story, and tentative deception means.

TECK: The core elements, *Technology, Emotion, Culture*, and *Knowledge*, unique to each individual, which influence perception in the *Observe* and *Orient* activity phases of the OODA Loop, and therefore, influence decision-making in the *Decide* and *Act* activity phases.